Limits of Black-Box Anamorphic Encryption

Dario Catalano[1] Emanuele Giunta[2, 3] Francesco Migliaro[1]

[1]Università di Catania, Italy.

[2]IMDEA Software Institute, Madrid, Spain.

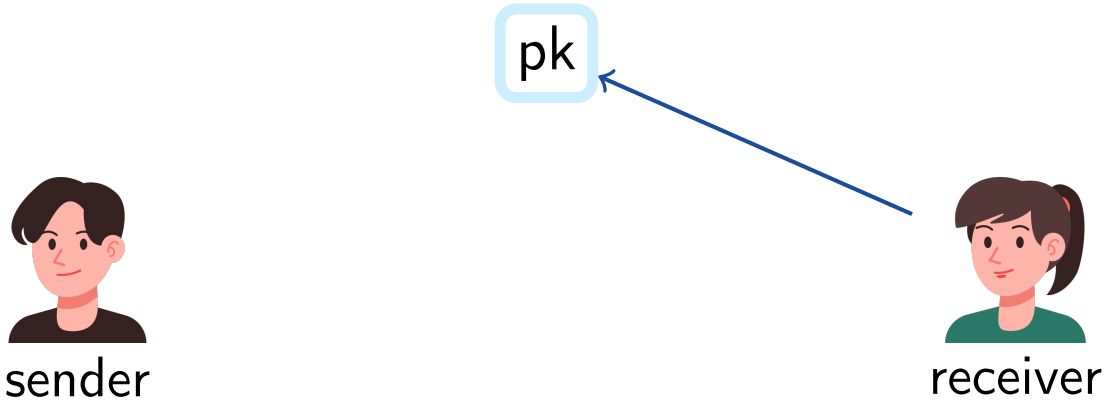
[3]Universidad Politecnica de Madrid, Spain.

Introduction

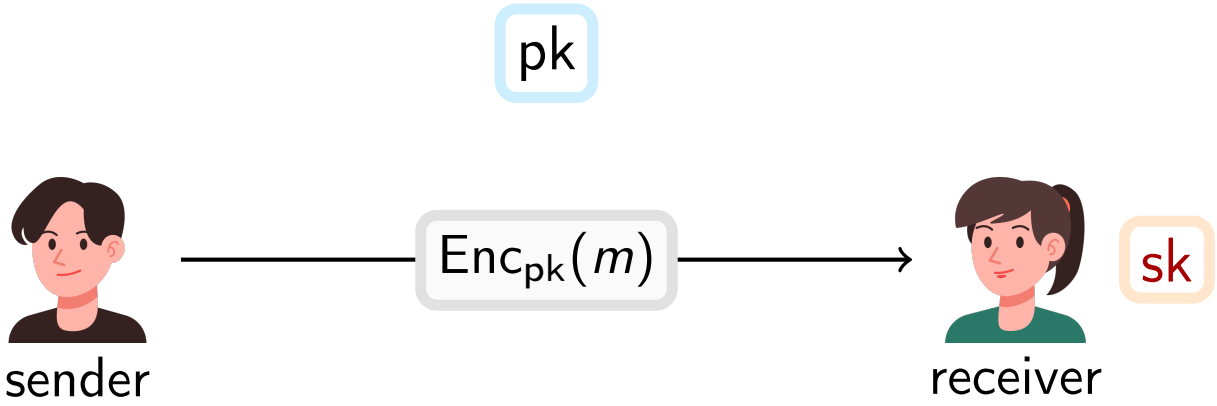
sender

receiver

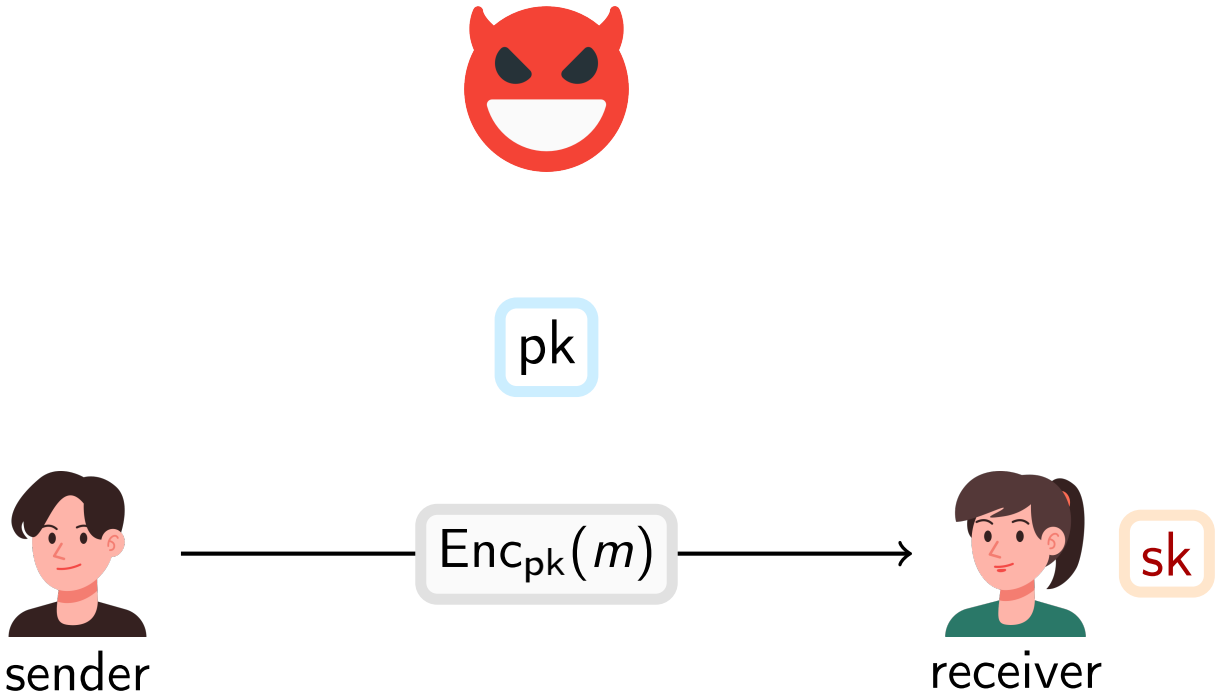
Introduction



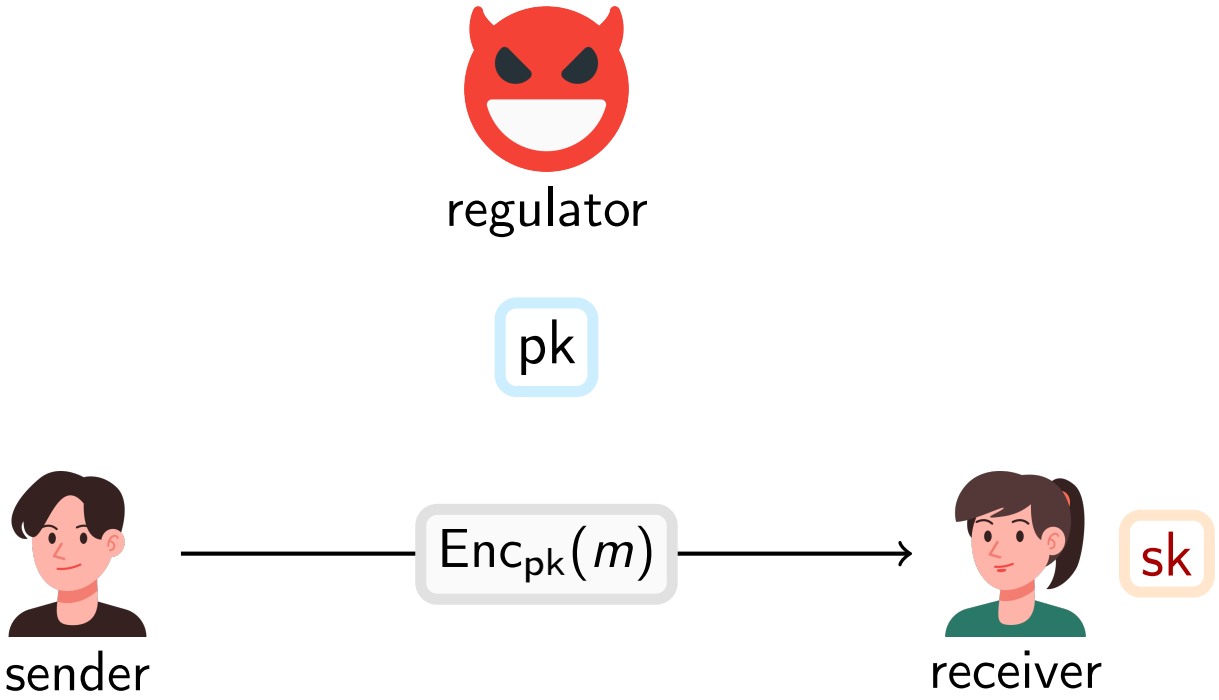
Introduction



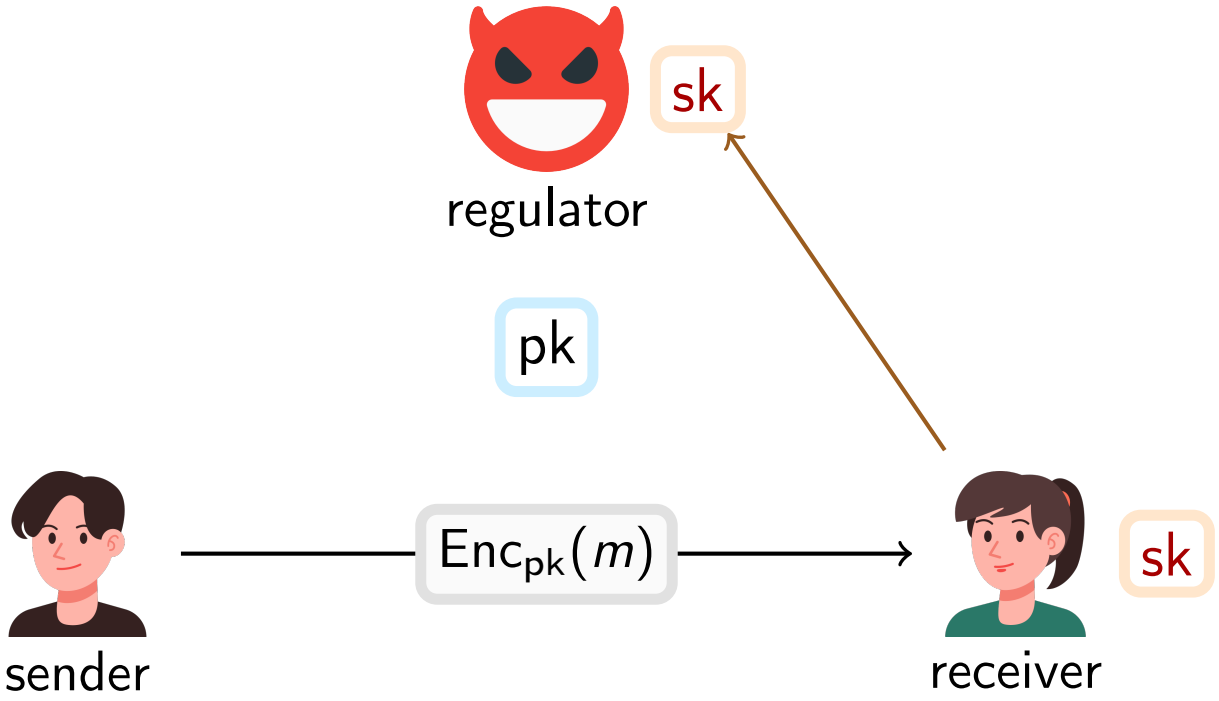
Introduction



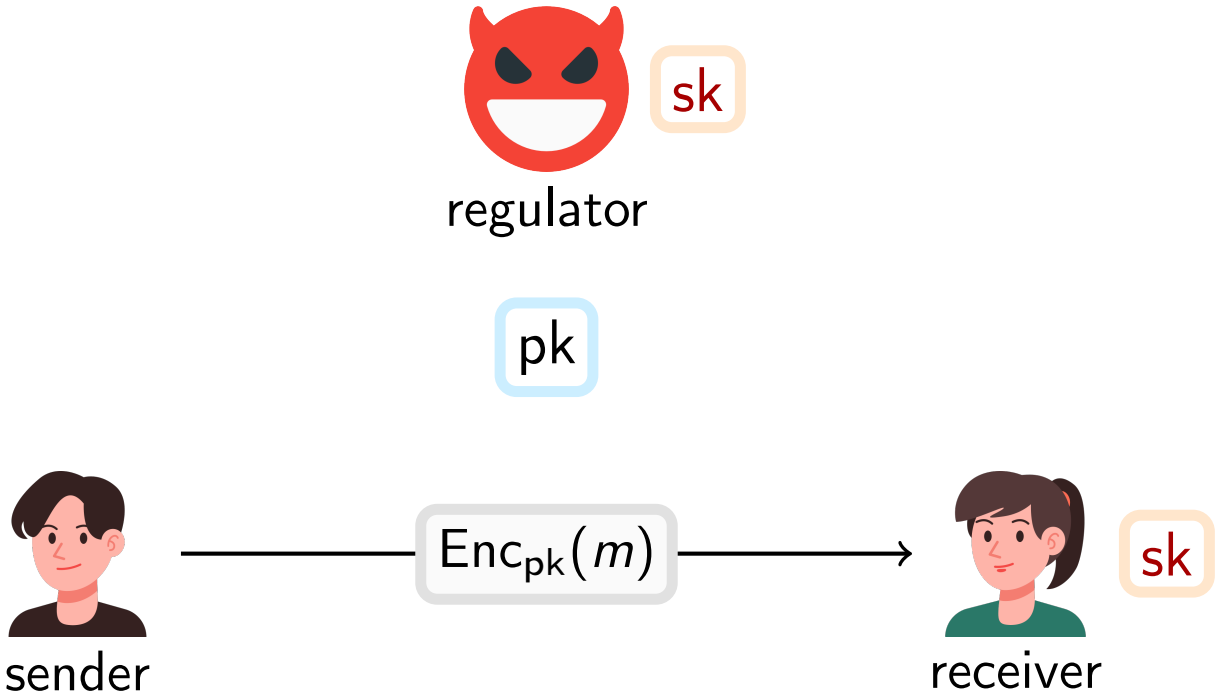
Introduction



Introduction



Introduction



Q. Can we have privacy from the regulator/dictator?

Anamorphic Encryption Definition [PPY22]

AT.Gen AT.Enc AT.Dec

Anamorphic Encryption Definition [PPY22]

AT.Gen AT.Enc AT.Dec

sender

receiver

regulator

Anamorphic Encryption Definition [PPY22]

AT.Gen AT.Enc AT.Dec

apk

dk

sender

ask
dk

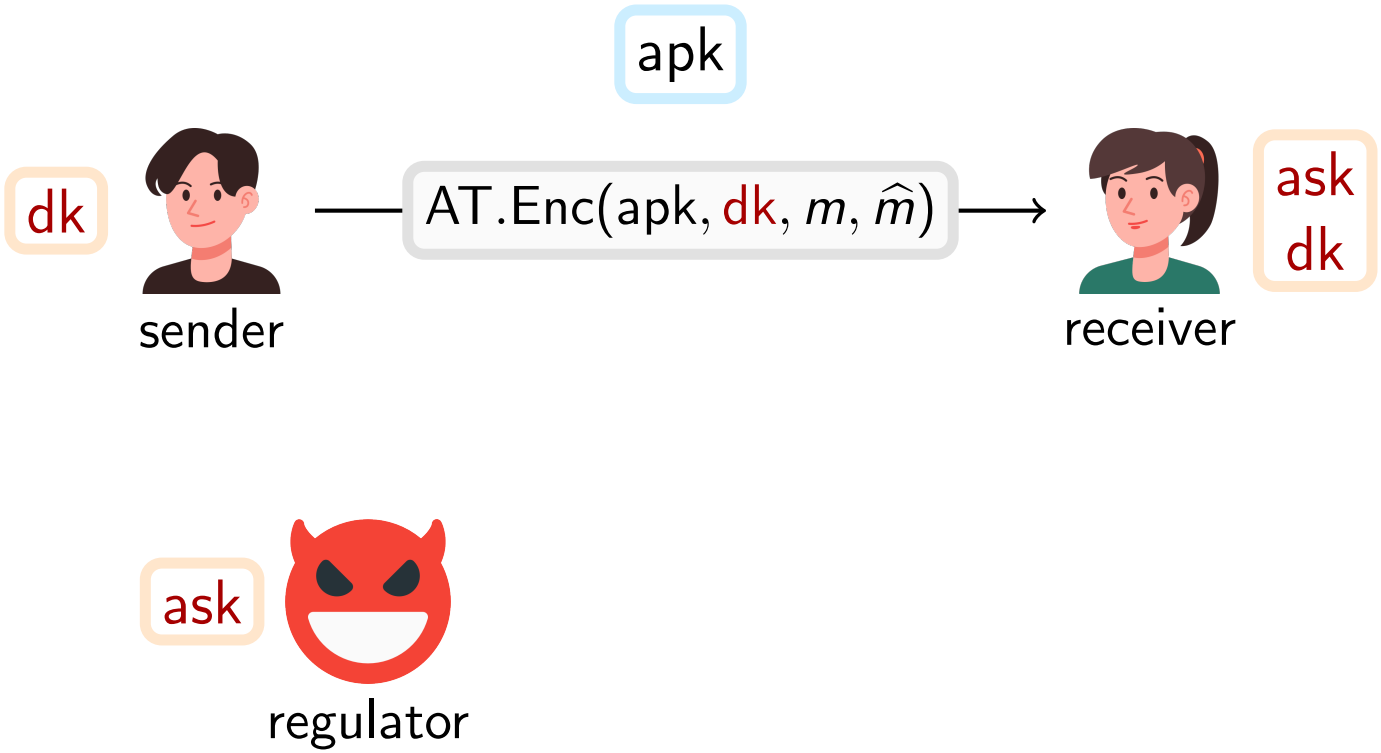
receiver

ask

regulator

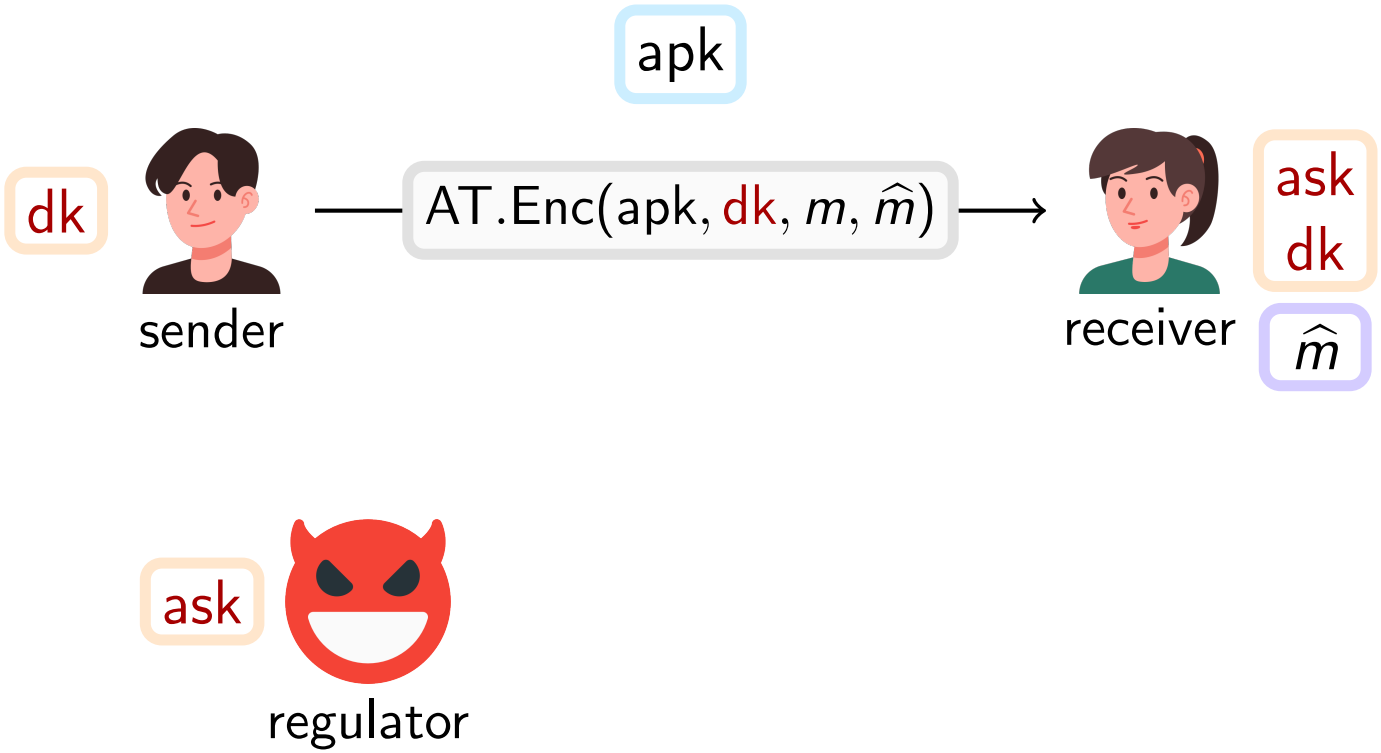
Anamorphic Encryption Definition [PPY22]

AT.Gen AT.Enc AT.Dec



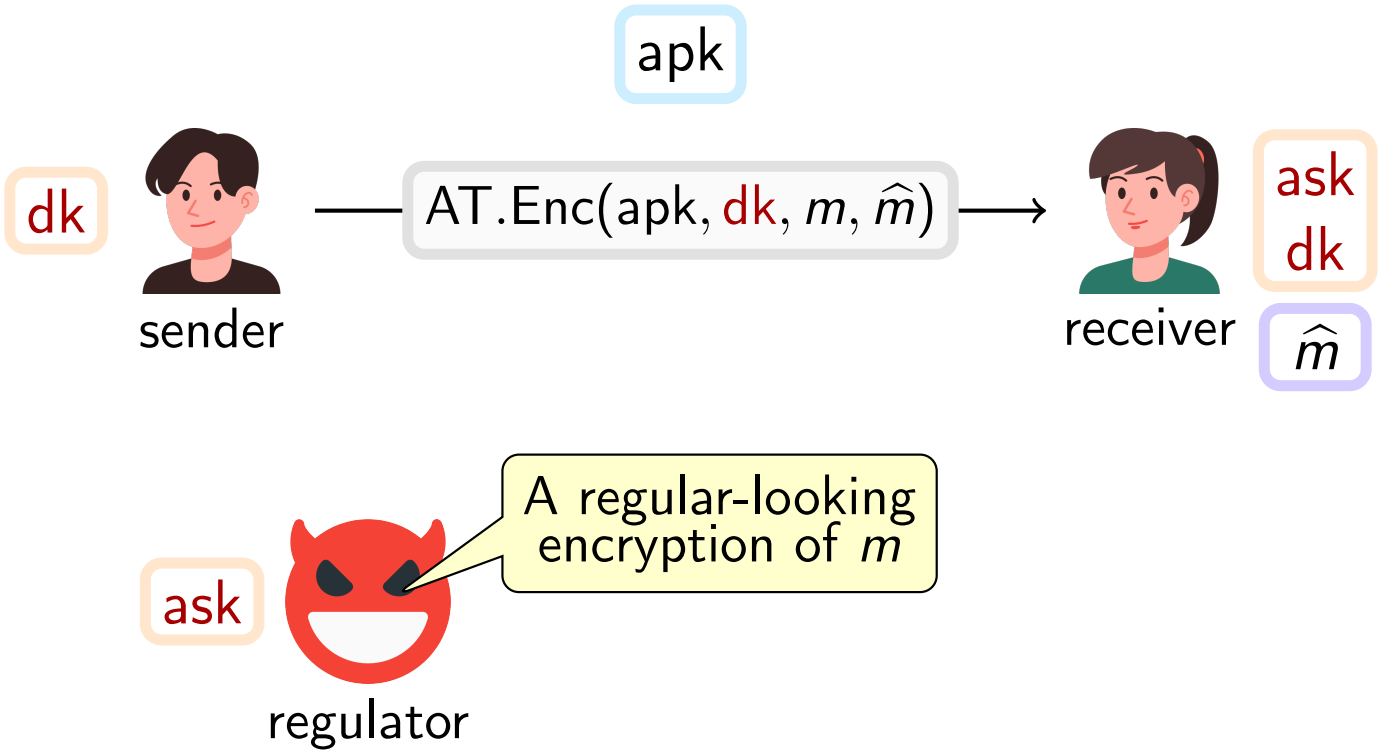
Anamorphic Encryption Definition [PPY22]

AT.Gen AT.Enc AT.Dec



Anamorphic Encryption Definition [PPY22]

AT.Gen AT.Enc AT.Dec

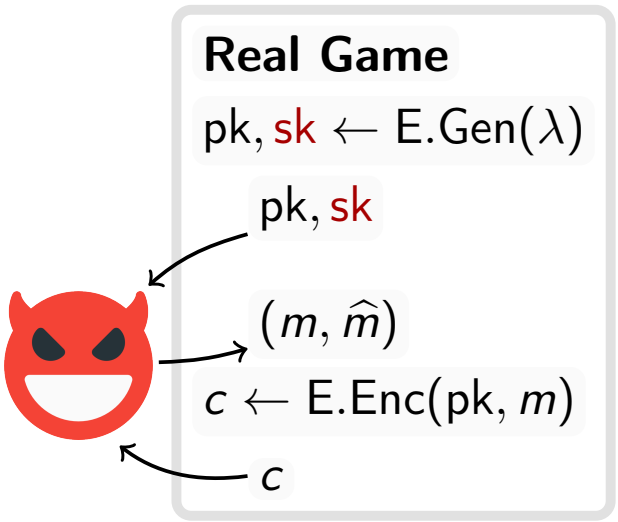


Anamorphic Encryption Definition [PPY22]

Security of an Anamorphic Triplet $(\mathsf{AT.Gen}, \mathsf{AT.Enc}, \mathsf{AT.Dec})$ is defined with respect to a PKE $(\mathsf{E.Gen}, \mathsf{E.Enc}, \mathsf{E.Dec})$.

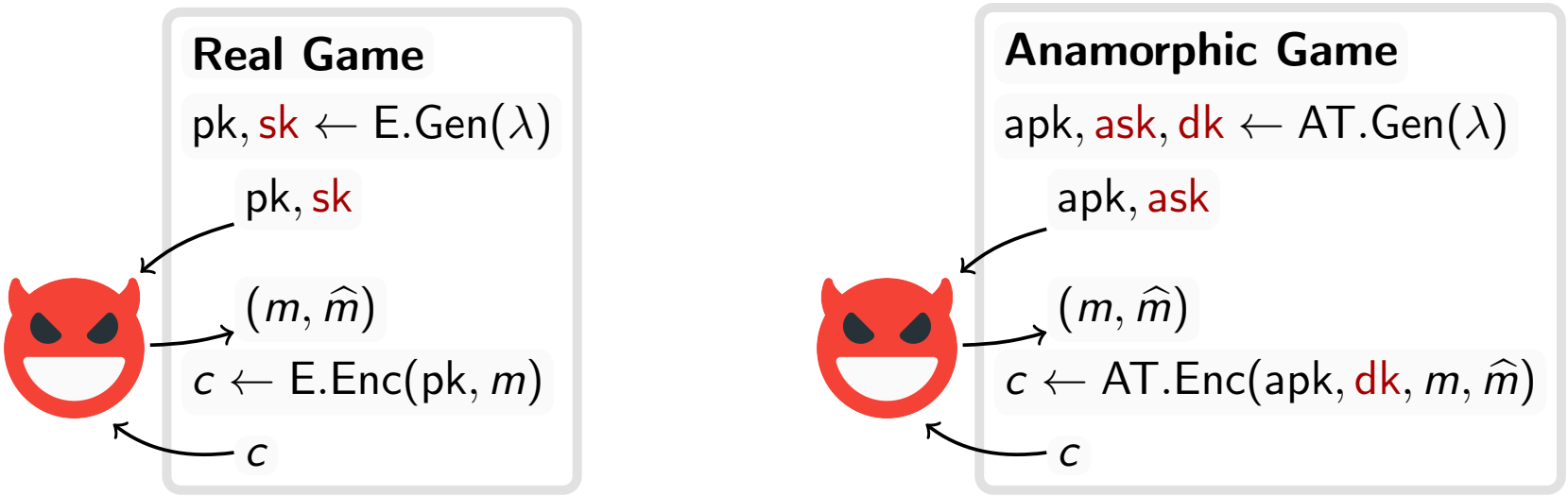
Anamorphic Encryption Definition [PPY22]

Security of an Anamorphic Triplet (AT.Gen, AT.Enc, AT.Dec) is defined with respect to a PKE (E.Gen, E.Enc, E.Dec).



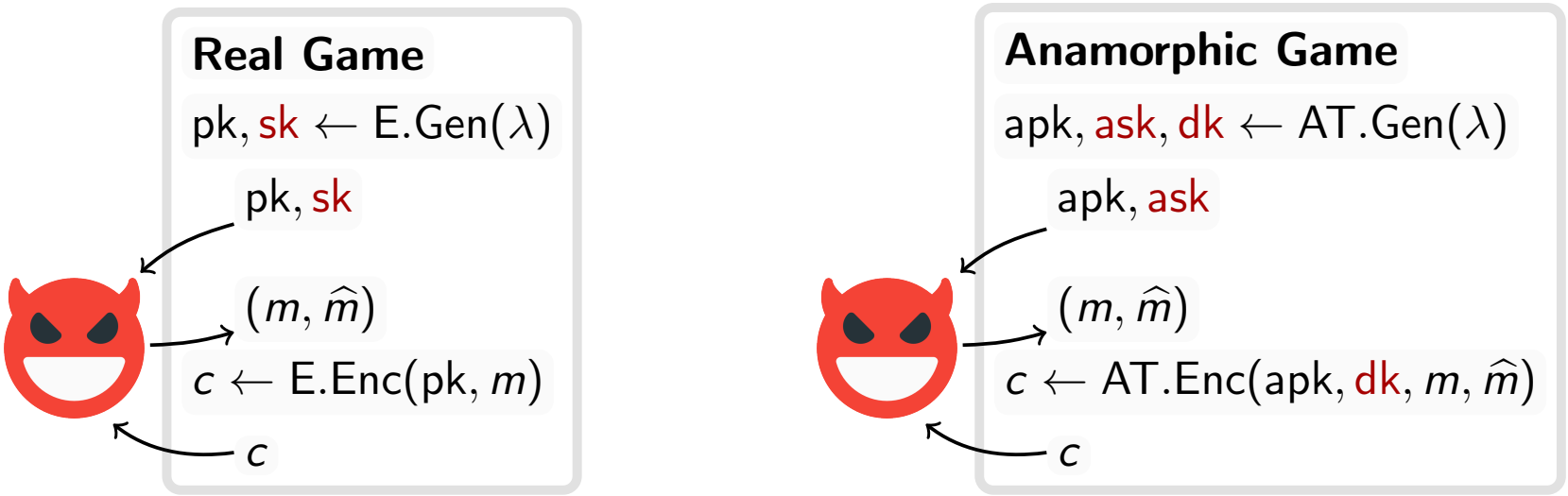
Anamorphic Encryption Definition [PPY22]

Security of an Anamorphic Triplet (AT.Gen, AT.Enc, AT.Dec) is defined with respect to a PKE (E.Gen, E.Enc, E.Dec).



Anamorphic Encryption Definition [PPY22]

Security of an Anamorphic Triplet (AT.Gen, AT.Enc, AT.Dec) is defined with respect to a PKE (E.Gen, E.Enc, E.Dec).



$$\textbf{Real Game} \overset{c}{\approx} \textbf{Anamorphic Game}$$

Constructions

Specific:

- Naor-Yung transform [PPY22]

Constructions

Specific:

- Naor-Yung transform [PPY22]
- Selective Randomness Recoverability [BGHM23, KPPY23]

Constructions

Specific:

- Naor-Yung transform [PPY22]
- Selective Randomness Recoverability [BGHM23, KPPY23]
- Hybrid Encryption [CGM24a]

Constructions

Specific:

- Naor-Yung transform [PPY22]
- Selective Randomness Recoverability [BGHM23, KPPY23]
- Hybrid Encryption [CGM24a]
- Specific schemes (e.g., ElGamal, Cramer-Shoup, GSW)

Constructions

Specific:

- Naor-Yung transform [PPY22]
- Selective Randomness Recoverability [BGHM23, KPPY23]
- Hybrid Encryption [CGM24a]
- Specific schemes (e.g., ElGamal, Cramer-Shoup, GSW)
- Reduction properties [PPY24]

Constructions

Specific:

- Naor-Yung transform [PPY22]
- Selective Randomness Recoverability [BGHM23, KPPY23]
- Hybrid Encryption [CGM24a]
- Specific schemes (e.g., ElGamal, Cramer-Shoup, GSW)
- Reduction properties [PPY24]

Generic:

Constructions

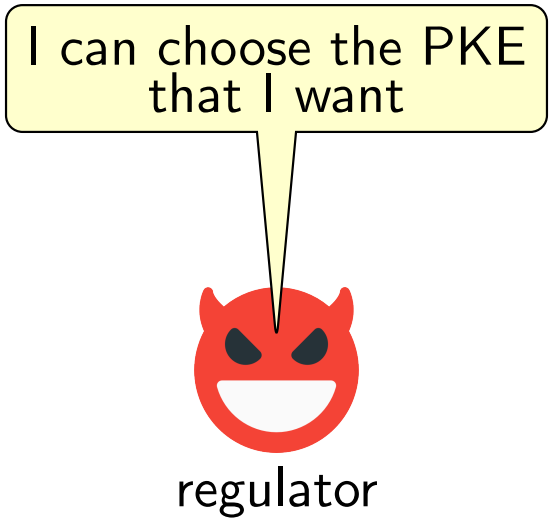
Specific:

- Naor-Yung transform [PPY22]
- Selective Randomness Recoverability [BGHM23, KPPY23]
- Hybrid Encryption [CGM24a]
- Specific schemes (e.g., ElGamal, Cramer-Shoup, GSW)
- Reduction properties [PPY24]

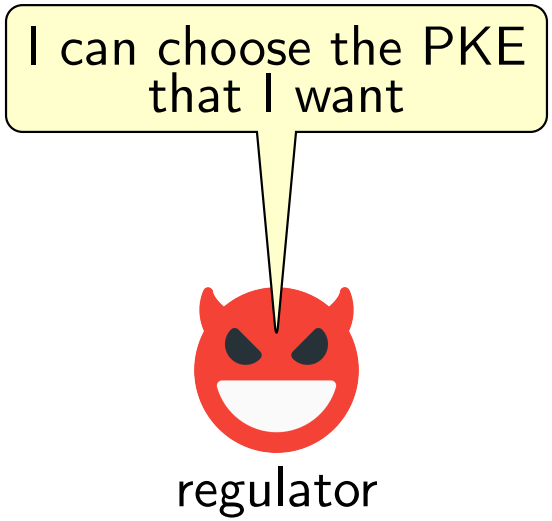
Generic:

- Rejection Sampling (RS) [PPY22] - Only $O(\log(\lambda))$ bits of communication

Question



Question



Q. For every PKE, what is the best that we can do? Is RS optimal?

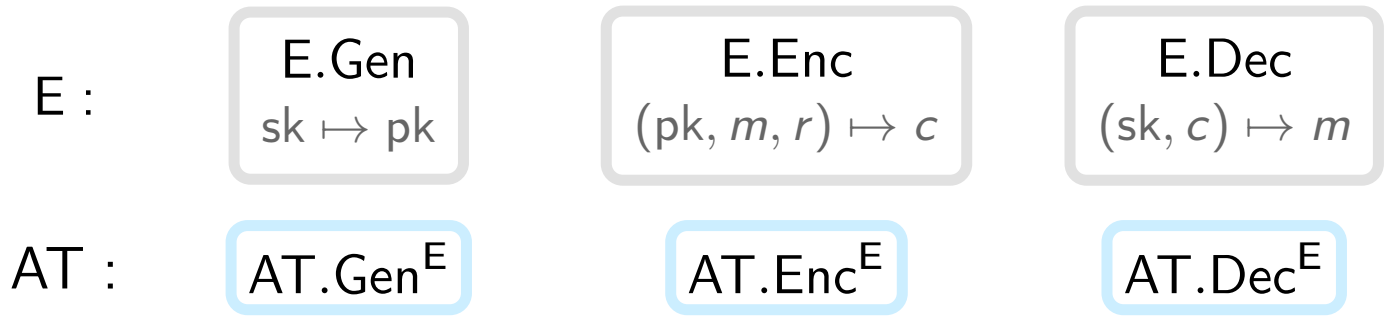
Black-Box Anamorphic Encryption

E : $\boxed{\text{E.Gen}\ \ \text{sk} \mapsto \text{pk}}$ $\boxed{\text{E.Enc}\ \ (\text{pk}, m, r) \mapsto c}$ $\boxed{\text{E.Dec}\ \ (\text{sk}, c) \mapsto m}$

Black-Box Anamorphic Encryption

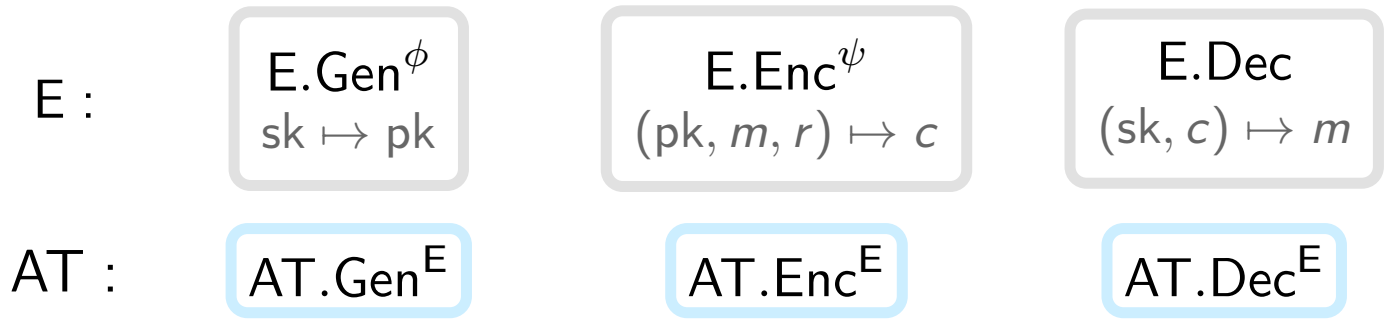
E :	E.Gen $\mathsf{sk} \mapsto \mathsf{pk}$	E.Enc $(\mathsf{pk}, m, r) \mapsto c$	E.Dec $(\mathsf{sk}, c) \mapsto m$
AT :	$\mathsf{AT.Gen}^{\mathsf{E}}$	$\mathsf{AT.Enc}^{\mathsf{E}}$	$\mathsf{AT.Dec}^{\mathsf{E}}$

Black-Box Anamorphic Encryption



Assumption: If the oracles in E form a correct and secure encryption scheme then $(\mathsf{E}, \mathsf{AT}^{\mathsf{E}})$ is a secure AE.

Black-Box Anamorphic Encryption



Assumption: If the oracles in E form a correct and secure encryption scheme then $(\mathsf{E}, \mathsf{AT}^{\mathsf{E}})$ is a secure AE.

Ideal PKE: Take E.Gen and E.Enc as truly random functions.

$$\phi : \mathsf{SK} \to \mathsf{PK} \qquad \psi : \mathsf{PK} \times M \times R \to C$$

Ciphertext Selection Lemma

$\mathsf{E.Gen}^{\phi}$
$\mathsf{sk} \mapsto \mathsf{pk}$

$\mathsf{E.Enc}^{\psi}$
$(\mathsf{pk}, m, r) \mapsto c$

$\mathsf{E.Dec}$
$(\mathsf{sk}, c) \mapsto m$

Ciphertext Selection Lemma

$\mathsf{E.Gen}^{\phi}$
$\mathsf{sk} \mapsto \mathsf{pk}$

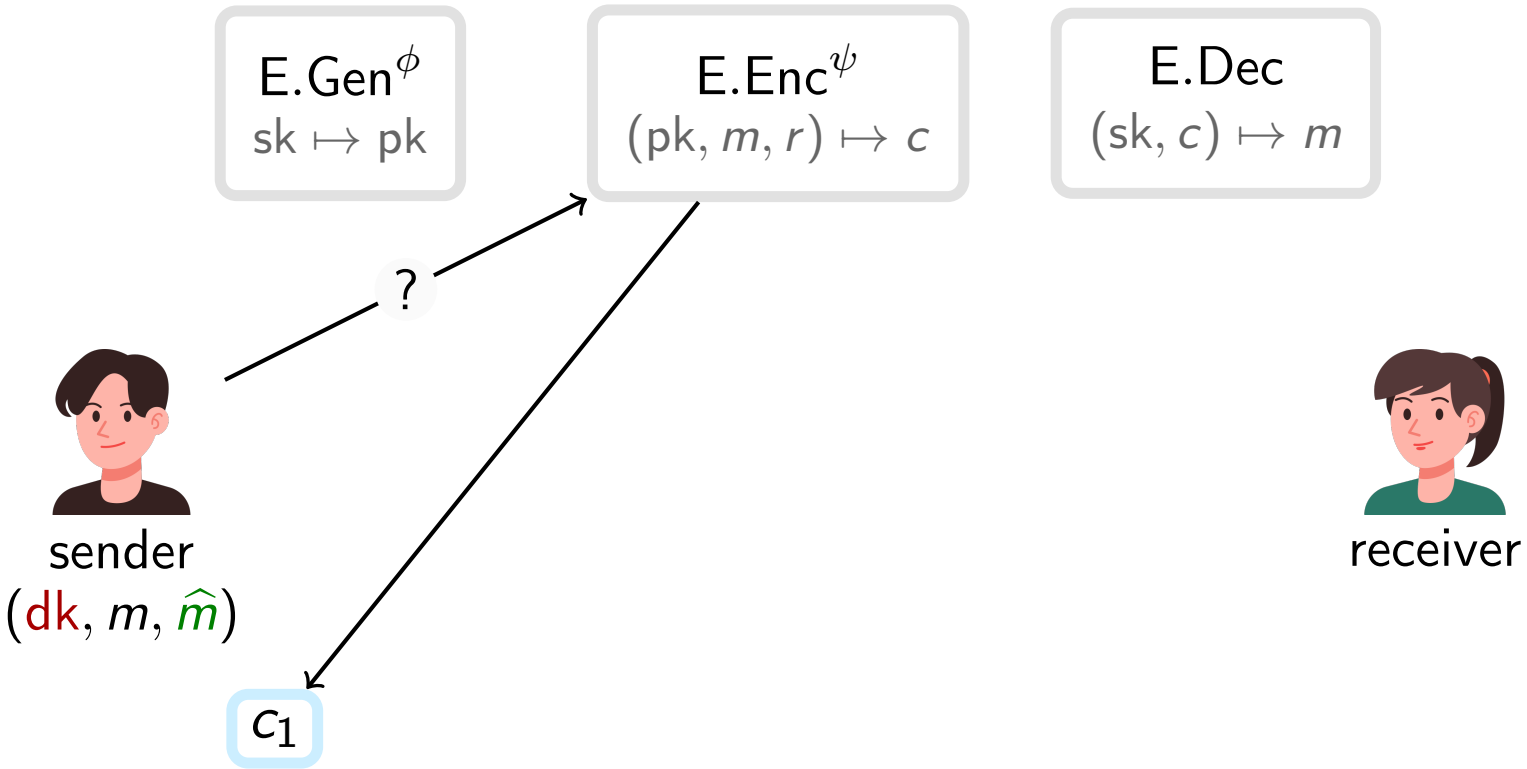
$\mathsf{E.Enc}^{\psi}$
$(\mathsf{pk}, m, r) \mapsto c$

$\mathsf{E.Dec}$
$(\mathsf{sk}, c) \mapsto m$

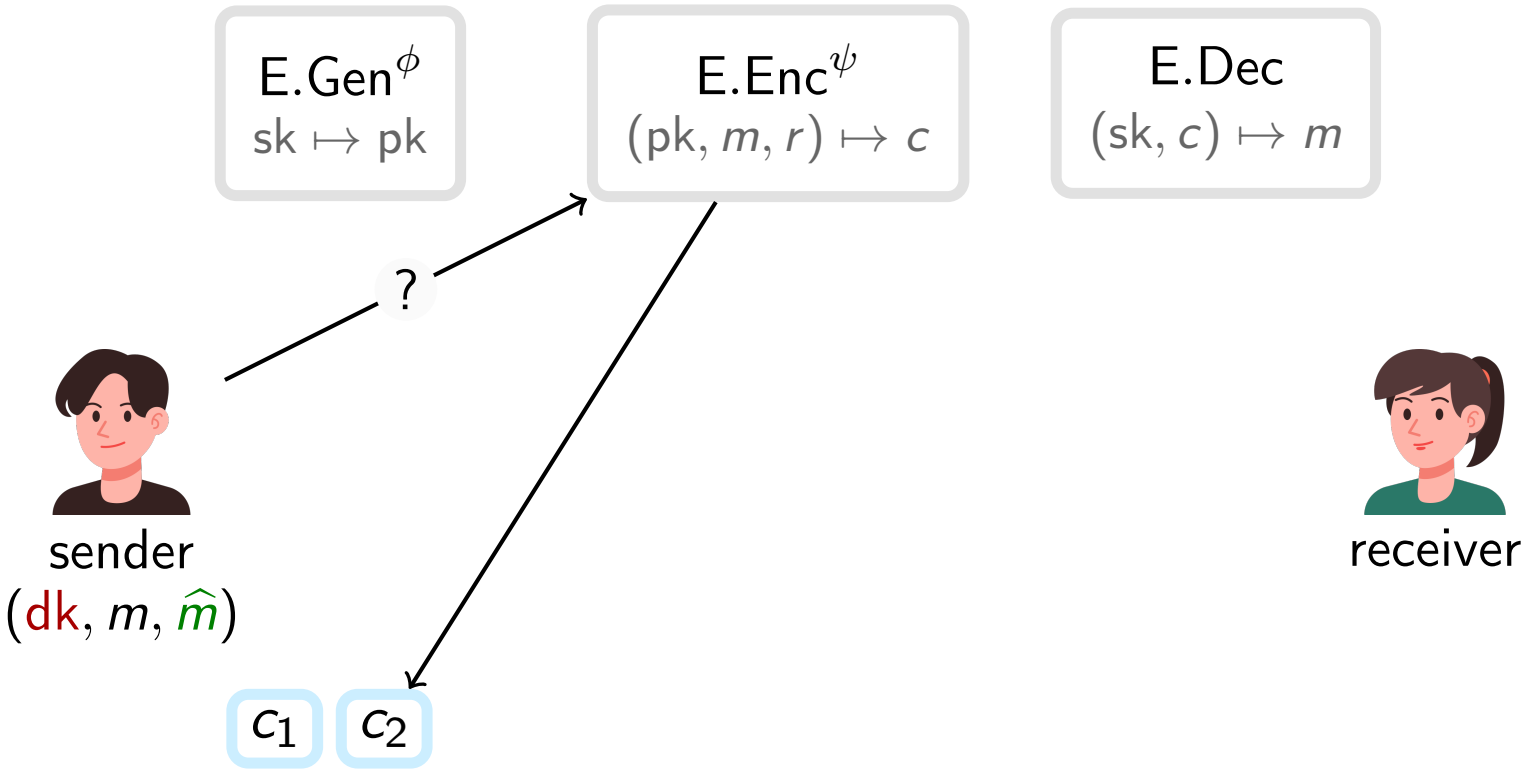
sender
$(\mathsf{dk}, m, \widehat{m})$

receiver

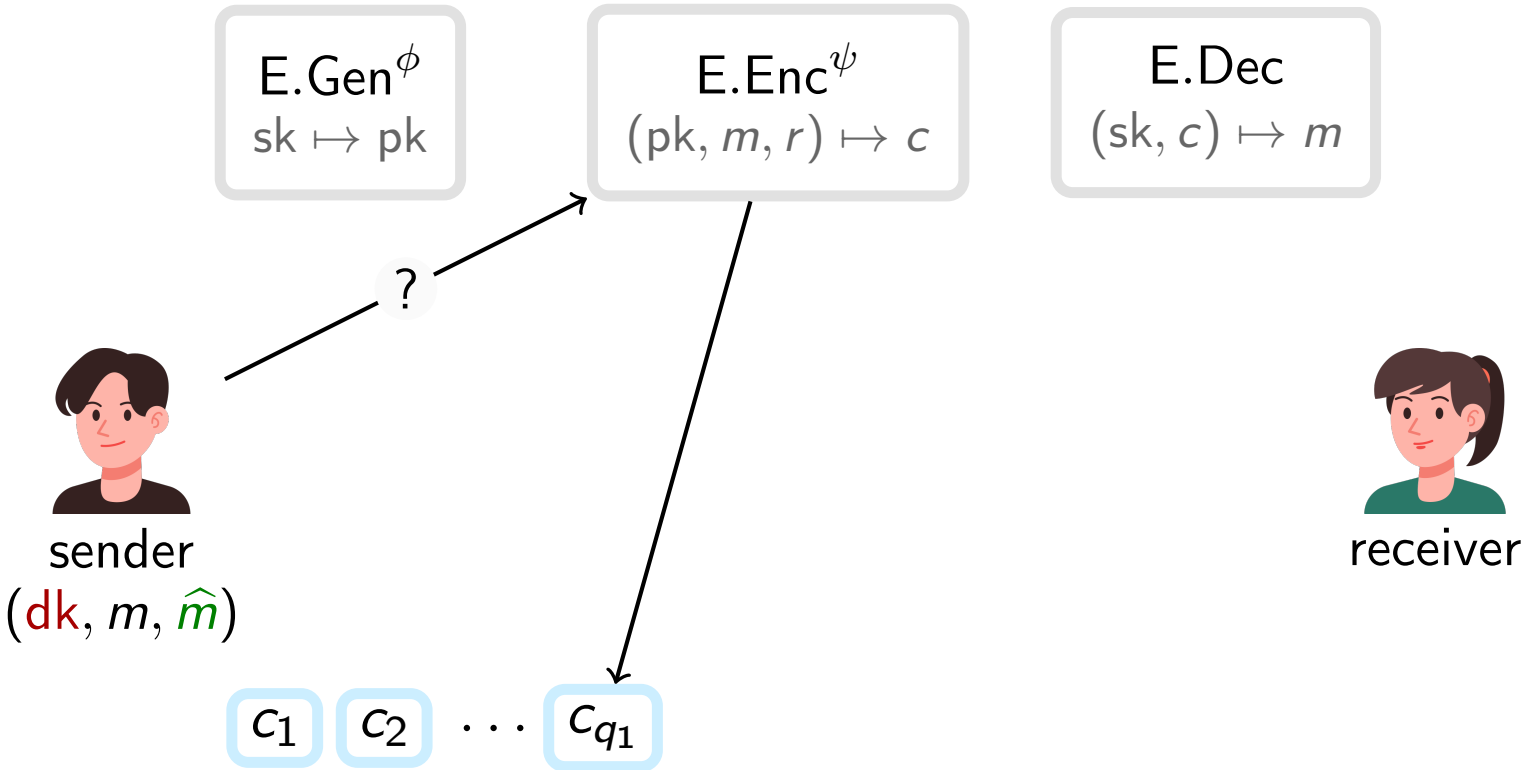
Ciphertext Selection Lemma



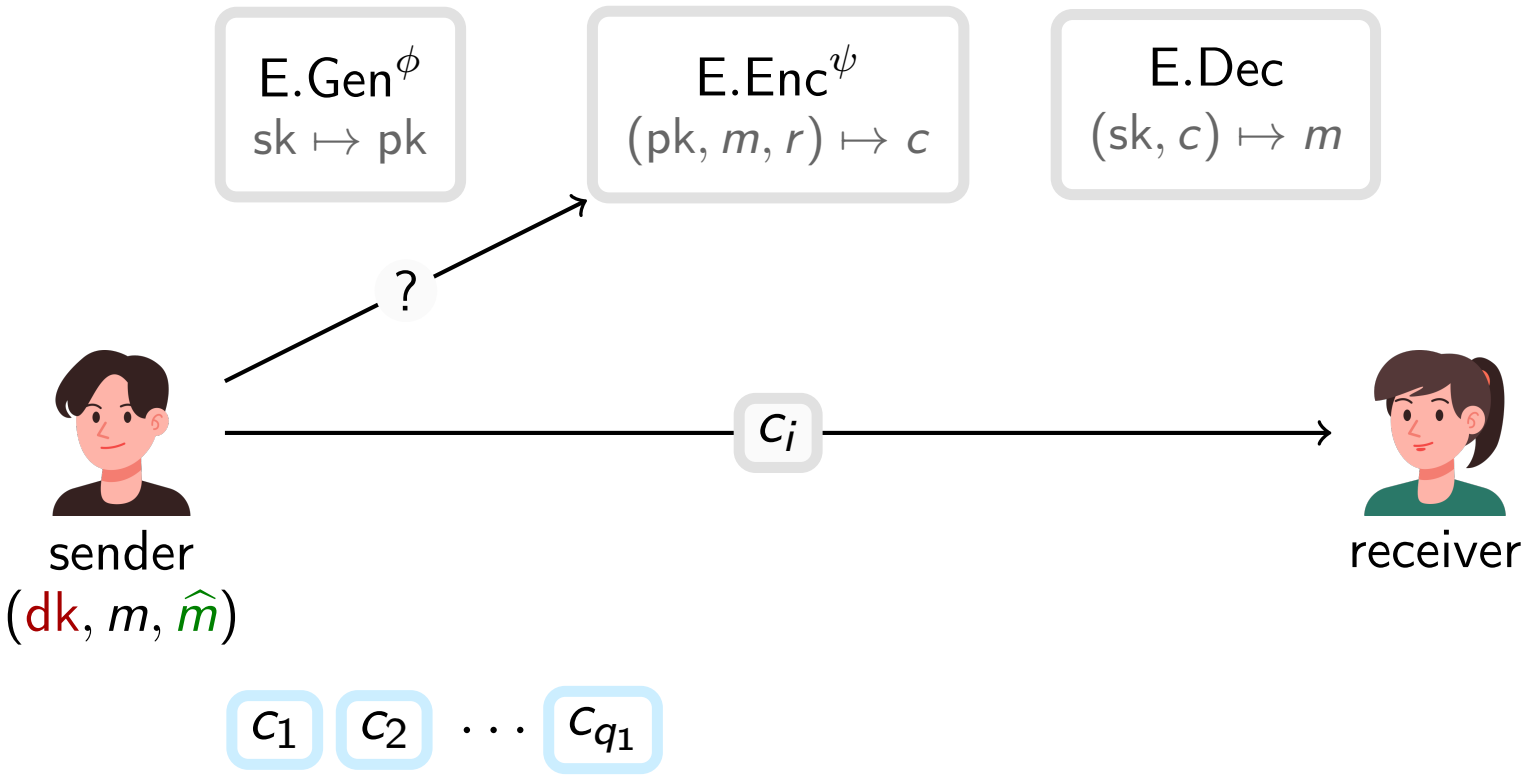
Ciphertext Selection Lemma



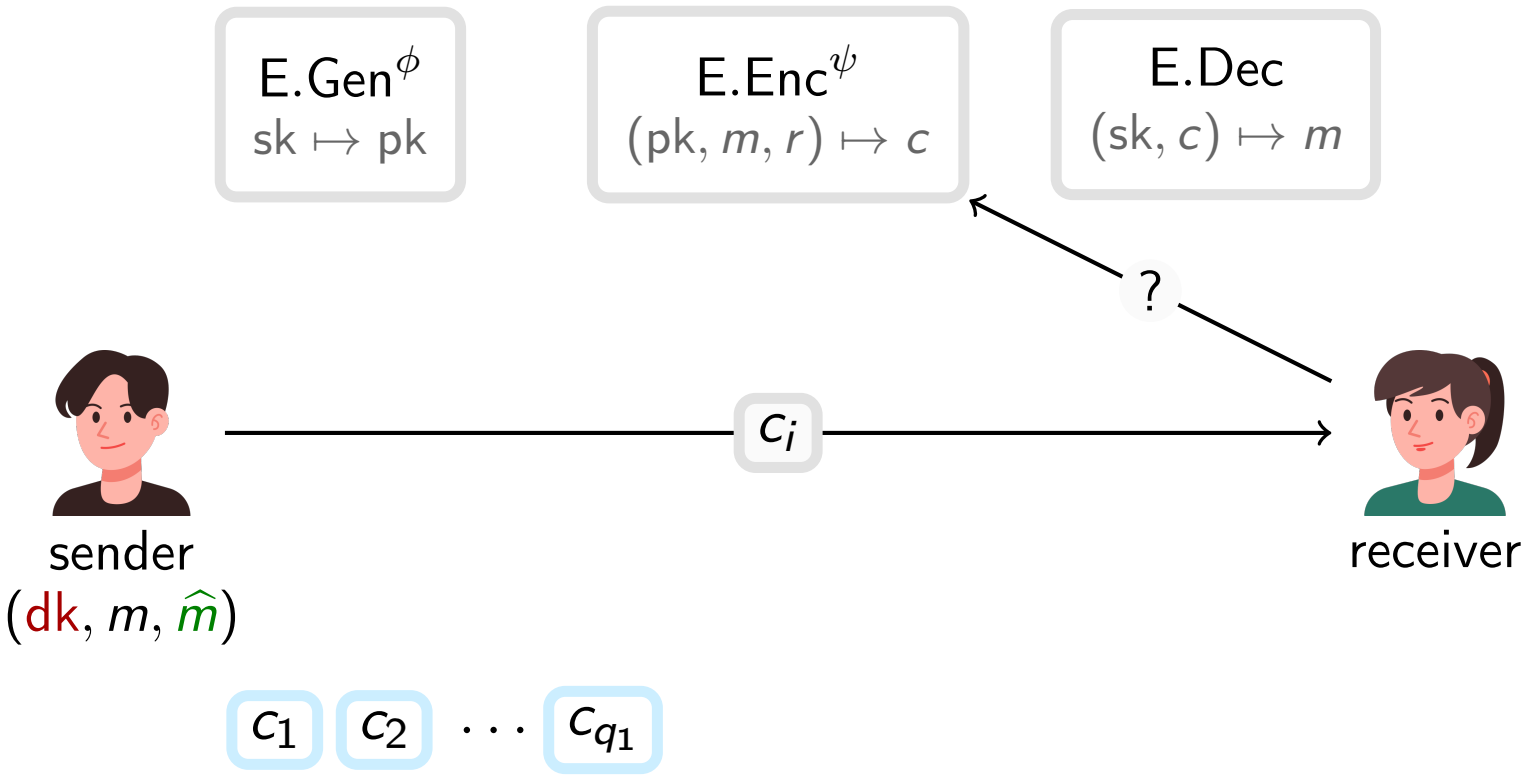
Ciphertext Selection Lemma



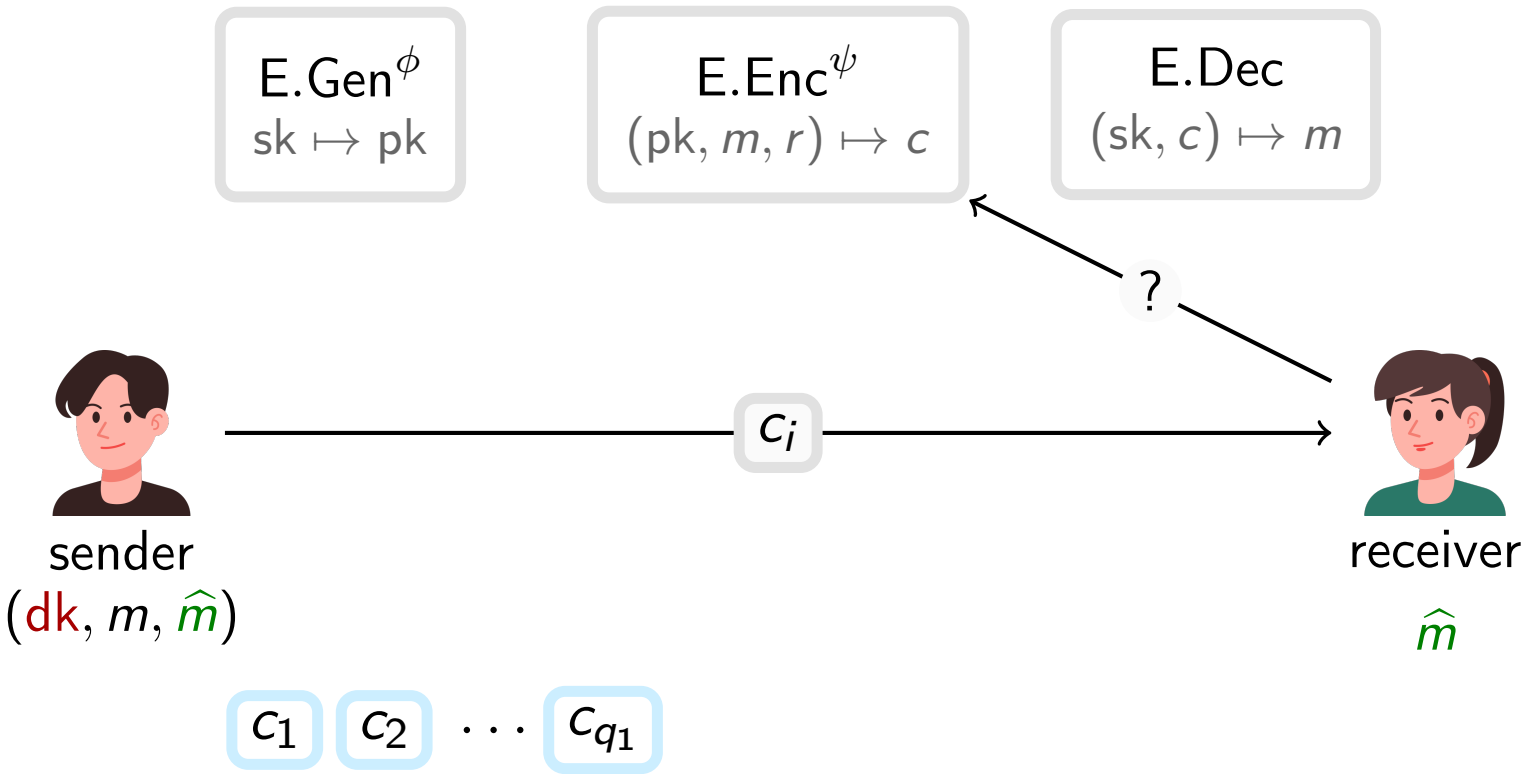
Ciphertext Selection Lemma



Ciphertext Selection Lemma



Ciphertext Selection Lemma



Random Oracle Channel - Definition

H

$x \mapsto y$

sender

receiver

Random Oracle Channel - Definition

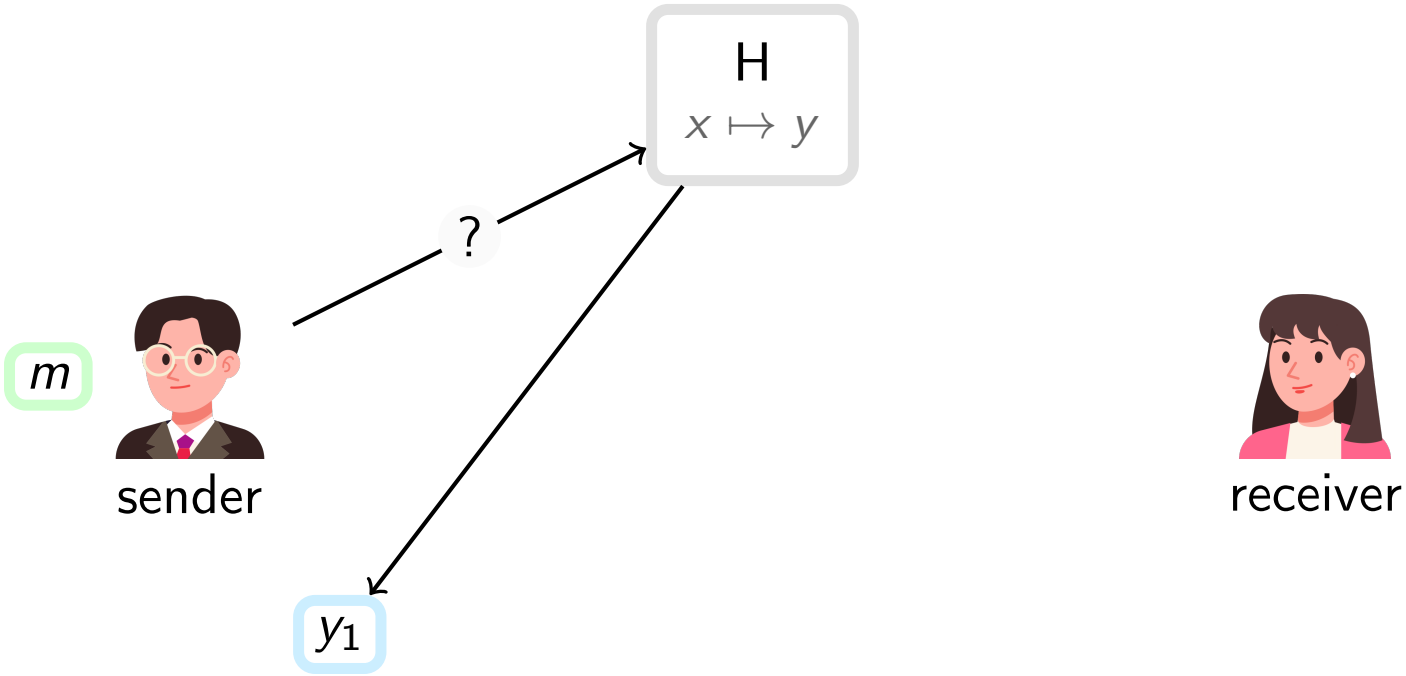
H
$x \mapsto y$

m

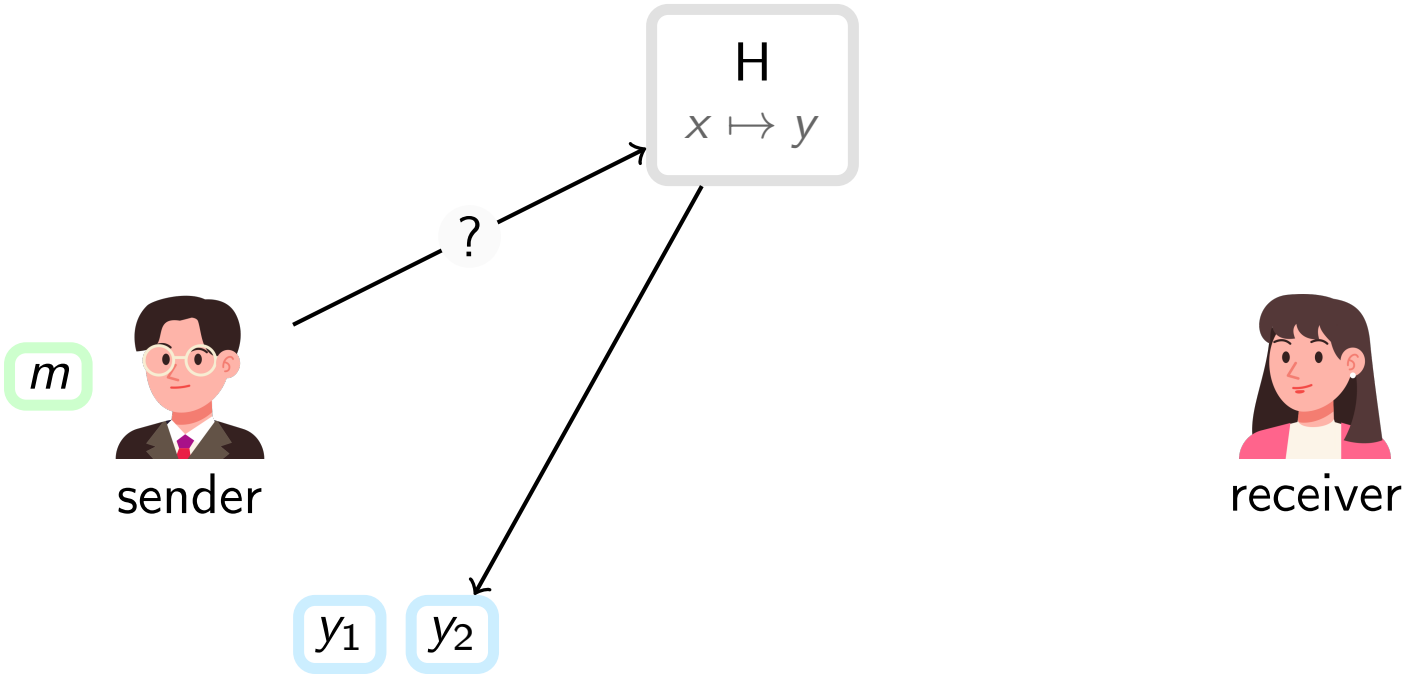
sender

receiver

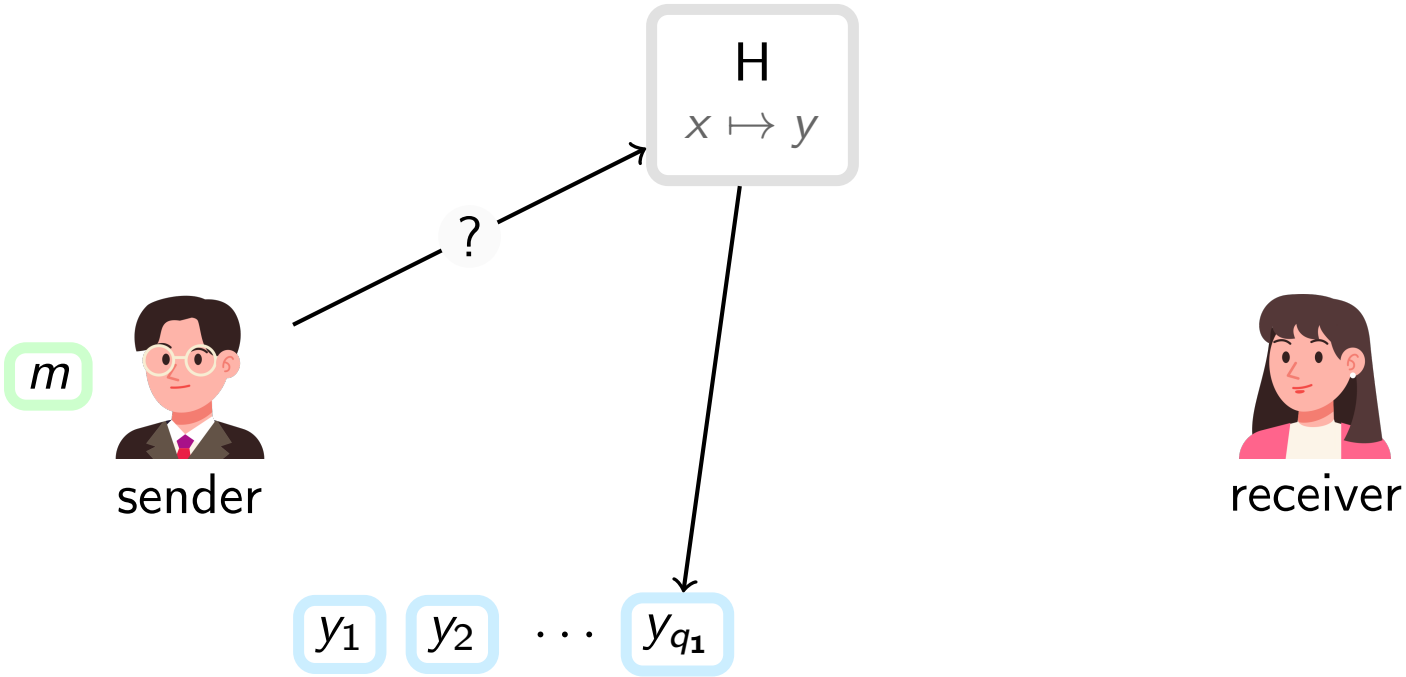
Random Oracle Channel - Definition



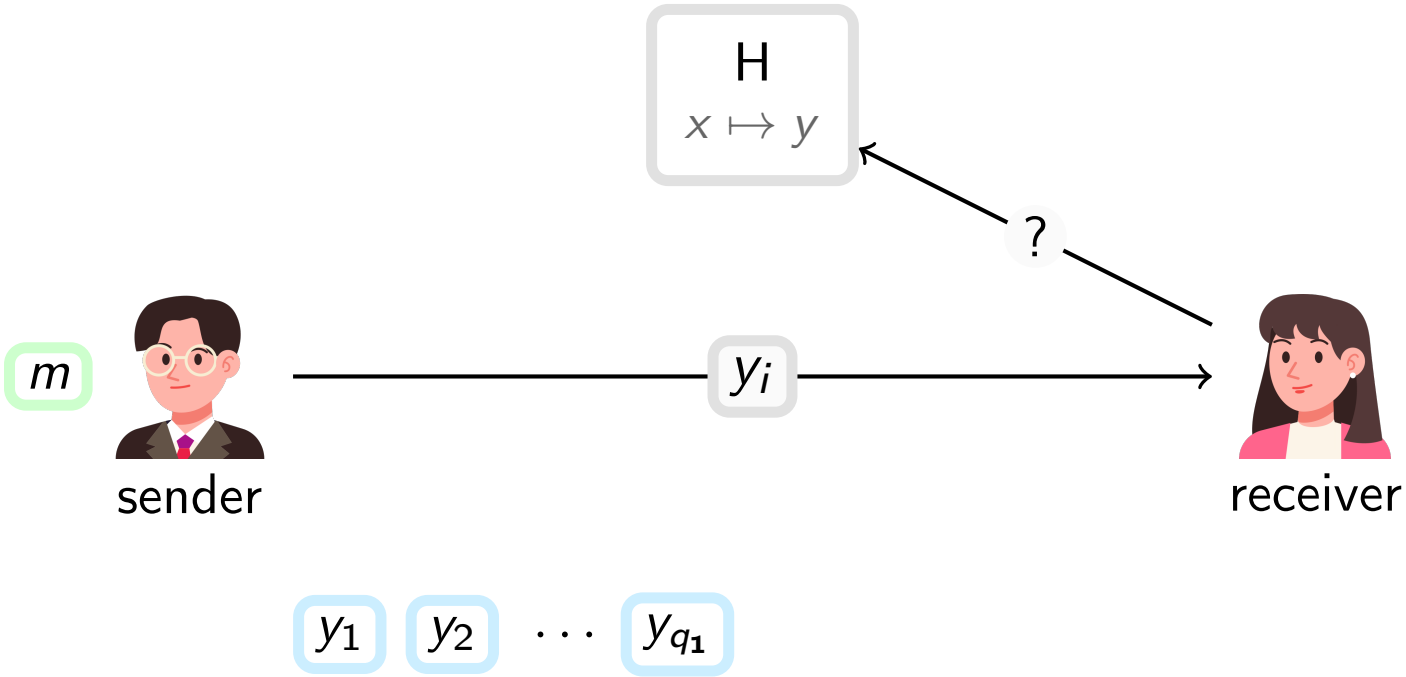
Random Oracle Channel - Definition



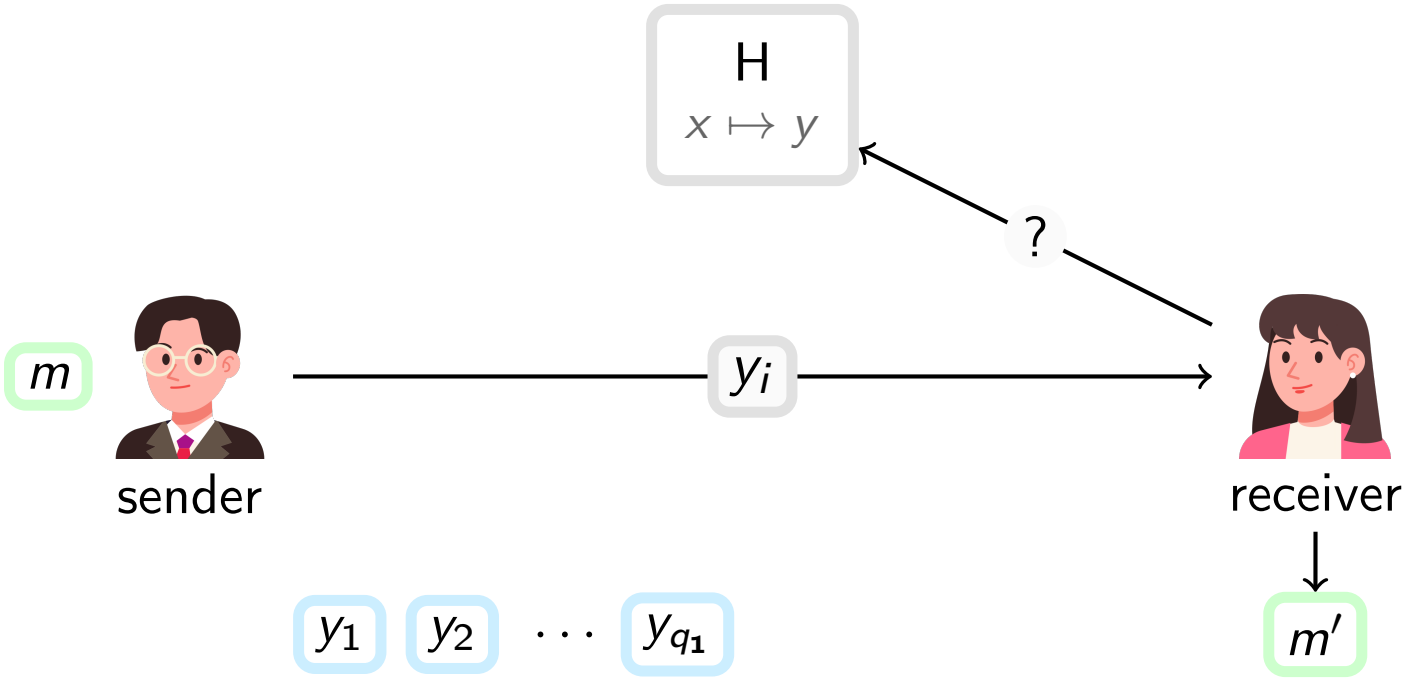
Random Oracle Channel - Definition



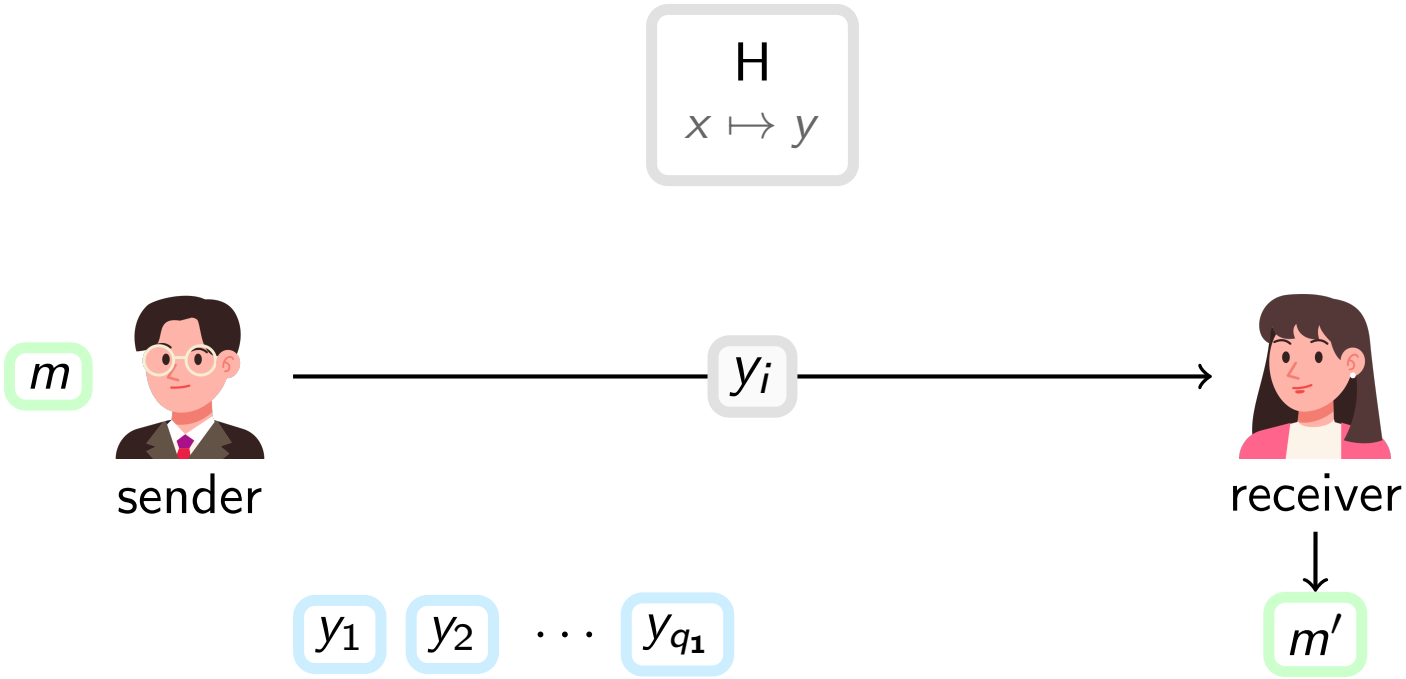
Random Oracle Channel - Definition



Random Oracle Channel - Definition



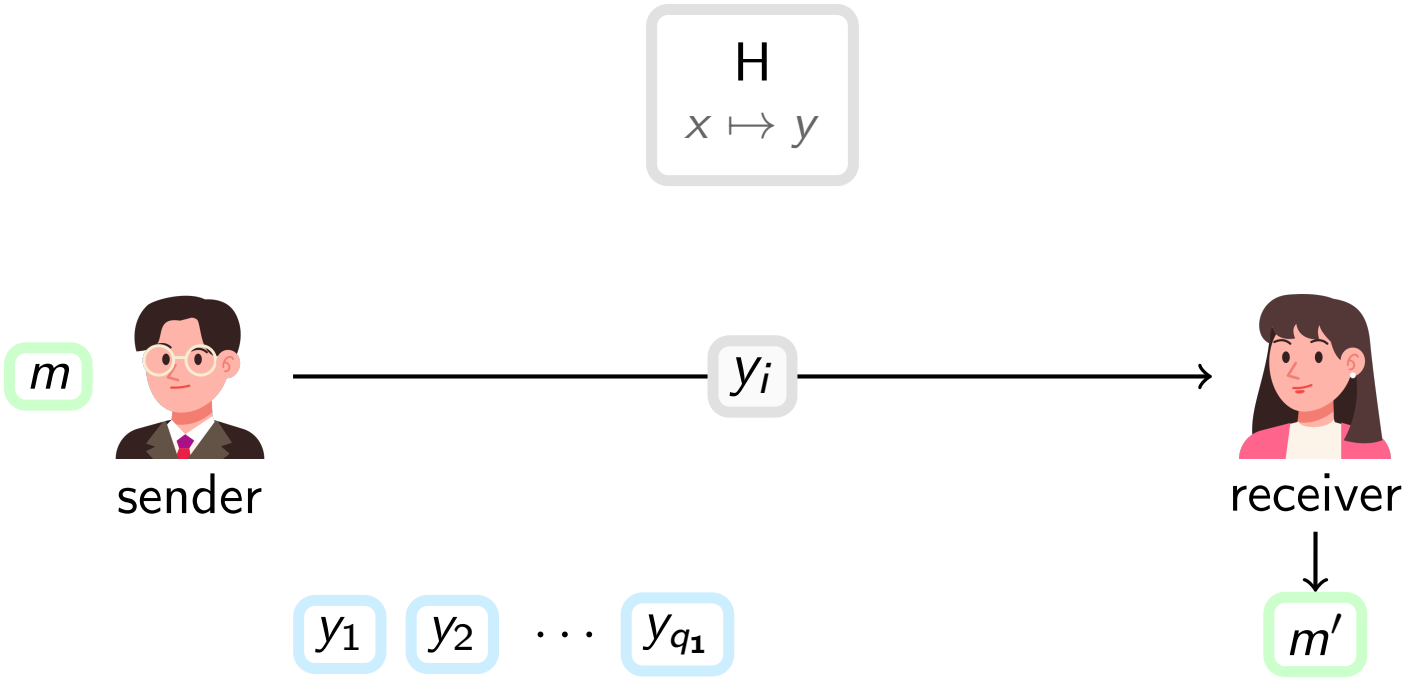
Random Oracle Channel - Definition



Efficiency: sender and receiver make resp. q_1 and q_2 queries with $q_1, q_2 = \text{poly}(\lambda)$.

Q. How many bit can they communicate?

Random Oracle Channel - Definition



Efficiency: sender and receiver make resp. q_1 and q_2 queries with $q_1, q_2 = \text{poly}(\lambda)$.

Q. How many bit can they communicate?

Our Bound: $|M| \leq 2(q_1 + q_2)^2$, i.e. $|m| \leq 2\log(q_1 + q_2) + 1$.

Random Oracle Channel - Upper Bound for AE

$$\mathsf{E.Enc}(\mathsf{pk}, m; r) \approx \mathsf{H}(\mathsf{pk}|m|r)$$

Random Oracle Channel - Upper Bound for AE

$$\mathsf{E.Enc}(\mathsf{pk}, m; r) \approx \mathsf{H}(\mathsf{pk}|m|r)$$

sender

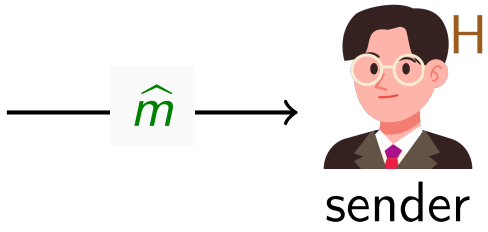
receiver

Random Oracle Channel - Upper Bound for AE

$$\mathsf{E.Enc}(\mathsf{pk}, m; r) \approx \mathsf{H}(\mathsf{pk}|m|r)$$

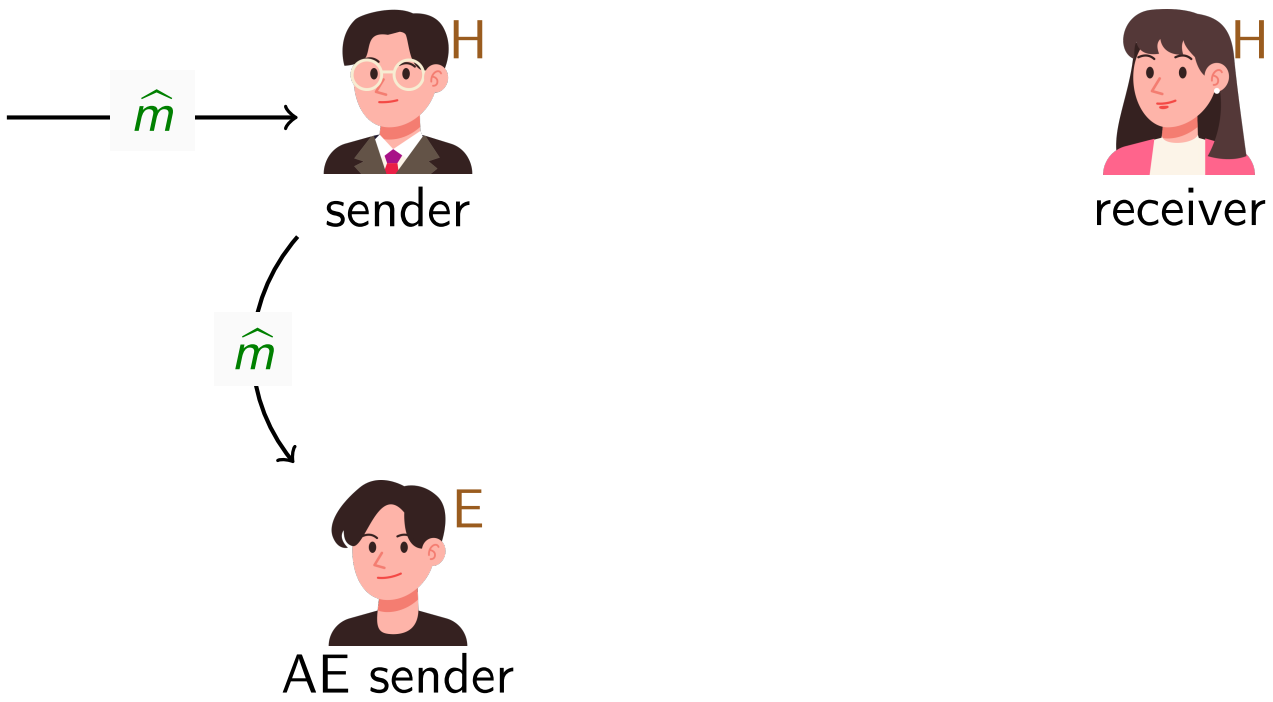
Random Oracle Channel - Upper Bound for AE

$$\mathsf{E.Enc}(\mathsf{pk}, m; r) \approx \mathsf{H}(\mathsf{pk}|m|r)$$



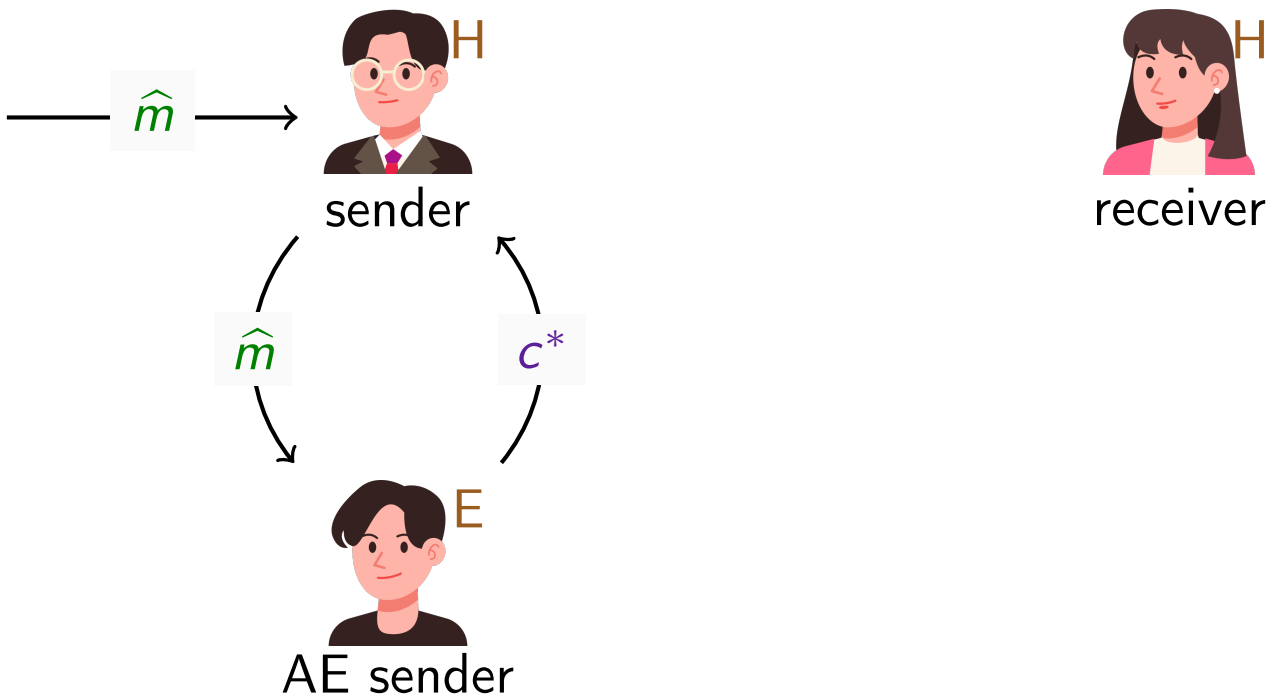
Random Oracle Channel - Upper Bound for AE

$$\mathsf{E.Enc}(\mathsf{pk}, m; r) \approx \mathsf{H}(\mathsf{pk}|m|r)$$



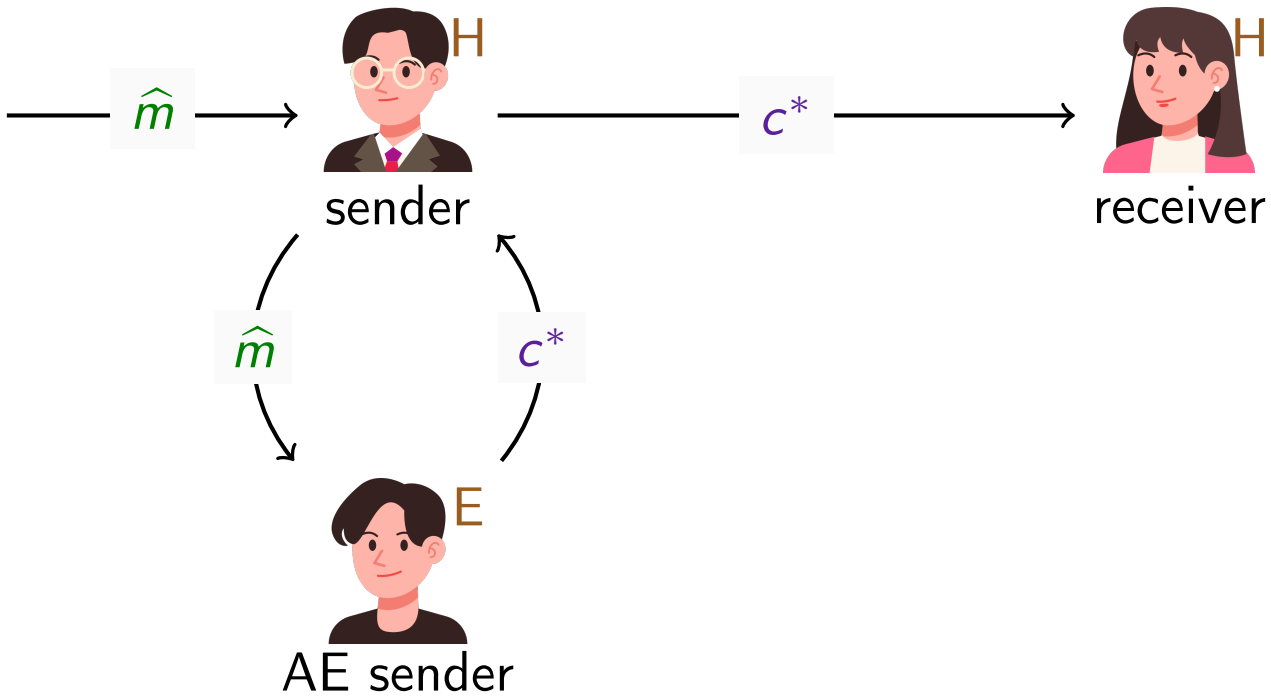
Random Oracle Channel - Upper Bound for AE

$$\mathsf{E.Enc}(\mathsf{pk}, m; r) \approx \mathsf{H}(\mathsf{pk}|m|r)$$



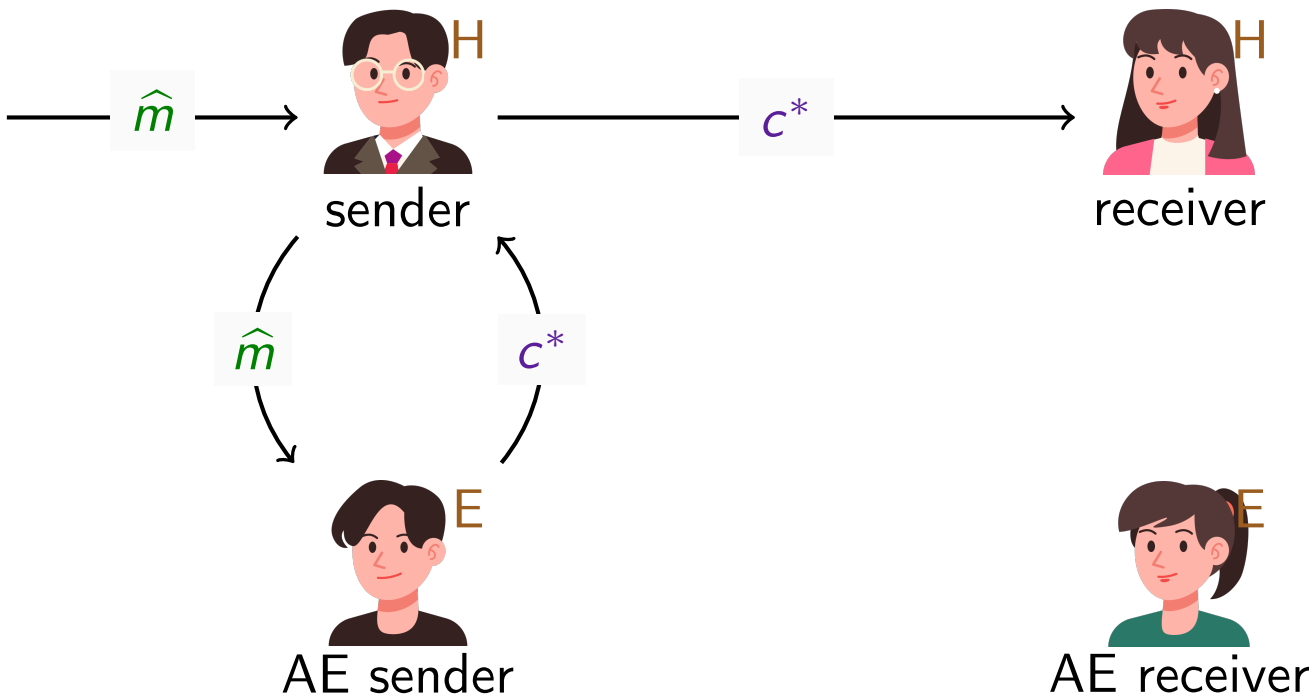
Random Oracle Channel - Upper Bound for AE

$$\mathsf{E.Enc}(\mathsf{pk}, m; r) \approx \mathsf{H}(\mathsf{pk}|m|r)$$



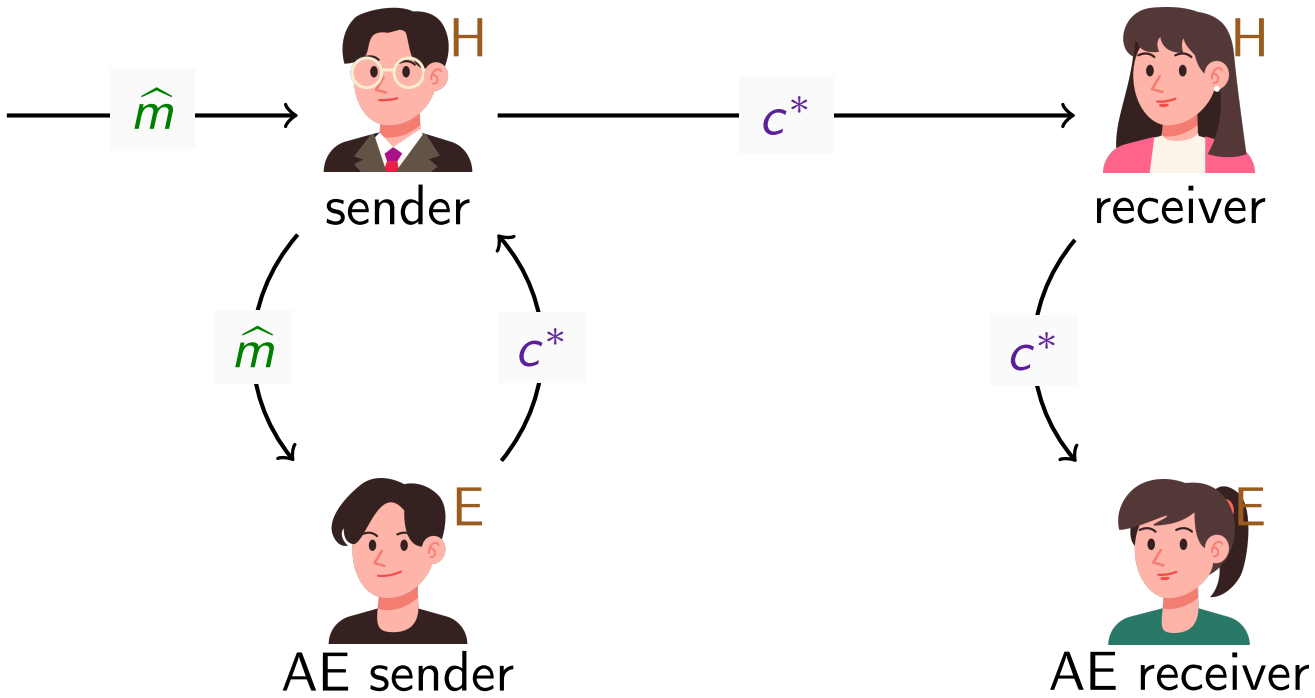
Random Oracle Channel - Upper Bound for AE

$$\mathsf{E.Enc}(\mathsf{pk}, m; r) \approx \mathsf{H}(\mathsf{pk}|m|r)$$



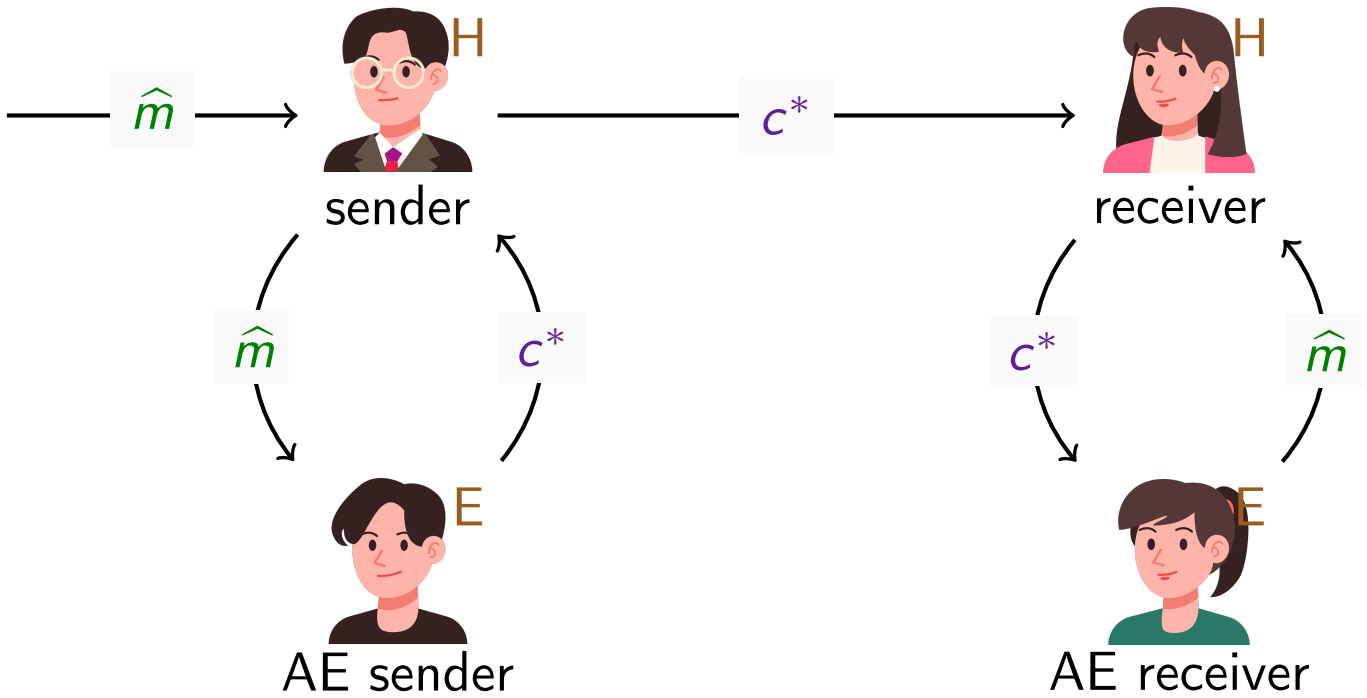
Random Oracle Channel - Upper Bound for AE

$$\mathsf{E.Enc}(\mathsf{pk}, m; r) \approx \mathsf{H}(\mathsf{pk}|m|r)$$



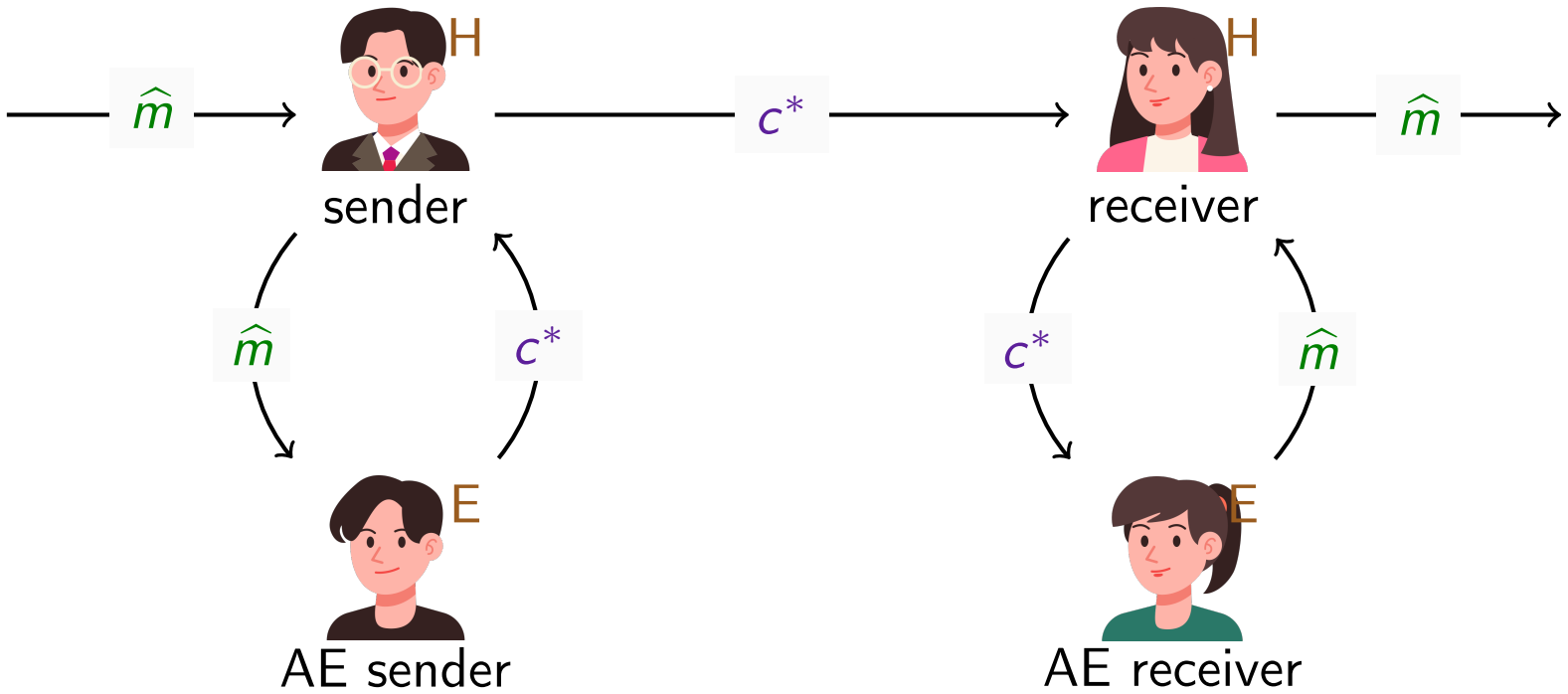
Random Oracle Channel - Upper Bound for AE

$$\mathsf{E.Enc}(\mathsf{pk}, m; r) \approx \mathsf{H}(\mathsf{pk}|m|r)$$



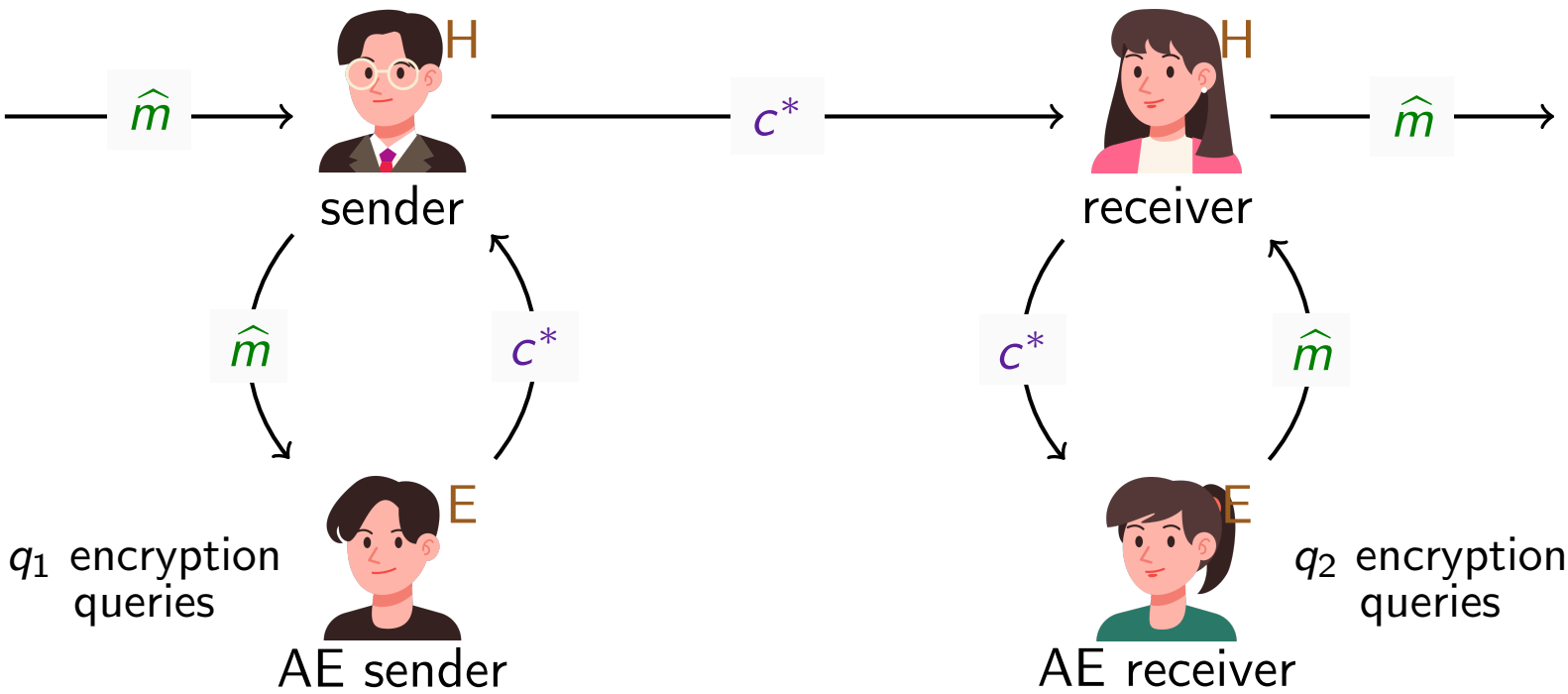
Random Oracle Channel - Upper Bound for AE

$$\mathsf{E.Enc}(\mathsf{pk}, m; r) \approx \mathsf{H}(\mathsf{pk}|m|r)$$



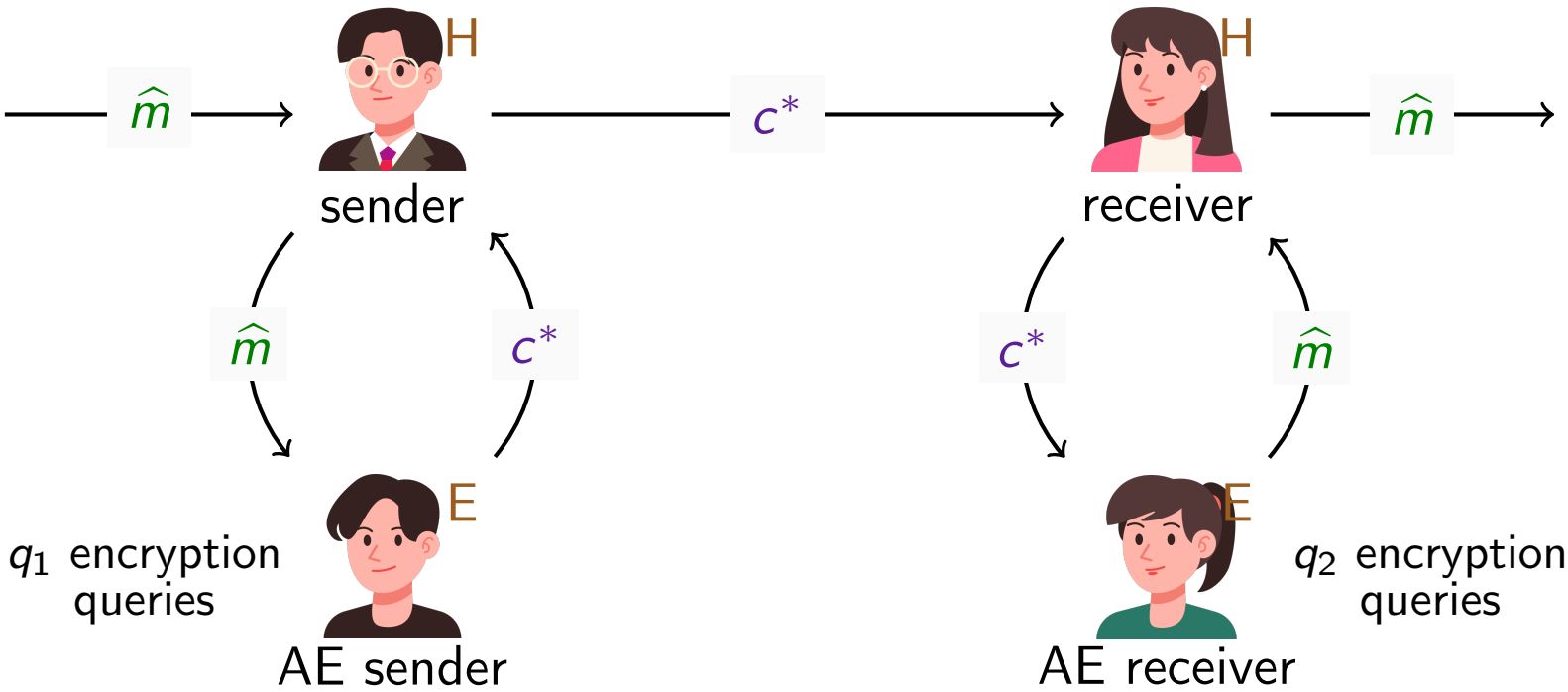
Random Oracle Channel - Upper Bound for AE

$$\text{E.Enc}(\text{pk}, m; r) \approx \text{H}(\text{pk}|m|r)$$



Random Oracle Channel - Upper Bound for AE

$$\boxed{\mathsf{E.Enc}(\mathsf{pk}, m; r)} \approx \boxed{\mathsf{H}(\mathsf{pk}|m|r)}$$



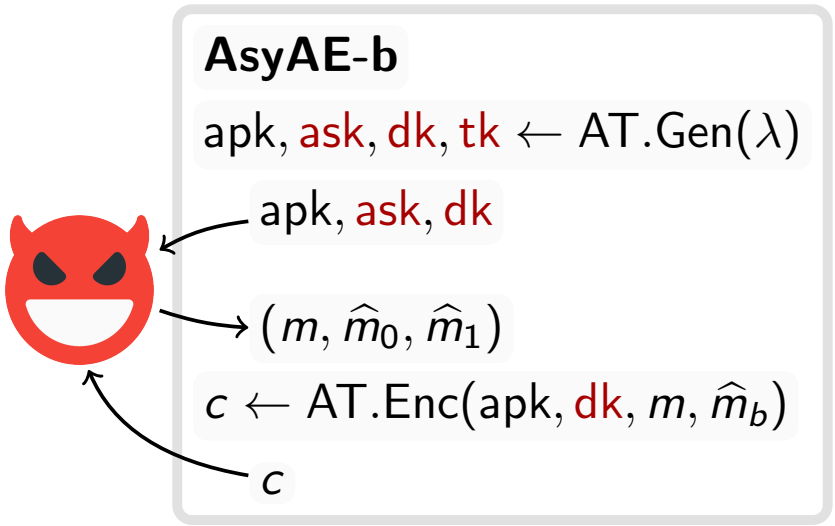
Therefore $|\widehat{m}| \leq 2\log(q_1 + q_2) + 1 = O(\log \lambda)$

Asymmetric AE Definition [CGM24a]

Security of Asymmetric AE $(\mathsf{AT.Gen}, \mathsf{AT.Enc}, \mathsf{AT.Dec})$ is defined with respect to a PKE $(\mathsf{E.Gen}, \mathsf{E.Enc}, \mathsf{E.Dec})$.

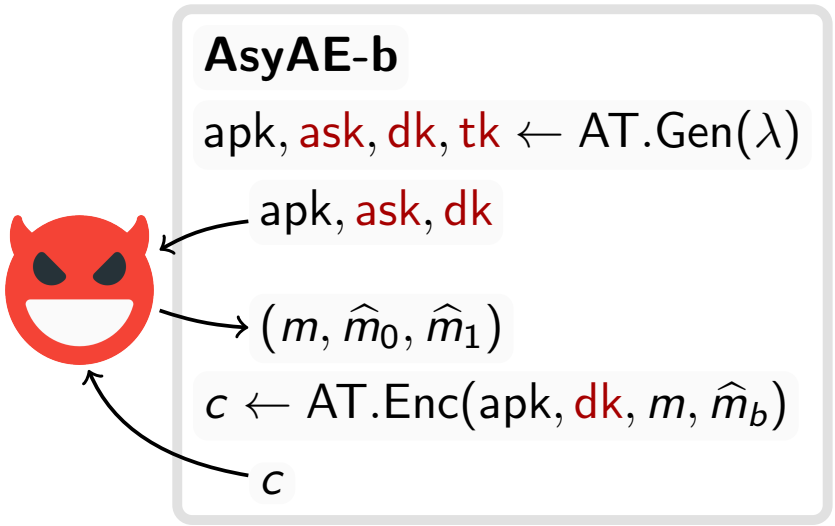
Asymmetric AE Definition [CGM24a]

Security of Asymmetric AE (AT.Gen, AT.Enc, AT.Dec) is defined with respect to a PKE (E.Gen, E.Enc, E.Dec).



Asymmetric AE Definition [CGM24a]

Security of Asymmetric AE (AT.Gen, AT.Enc, AT.Dec) is defined with respect to a PKE (E.Gen, E.Enc, E.Dec).



AsyAE-0 $\overset{c}{\approx}$ **AsyAE-1**.

Symmetric Choice Function

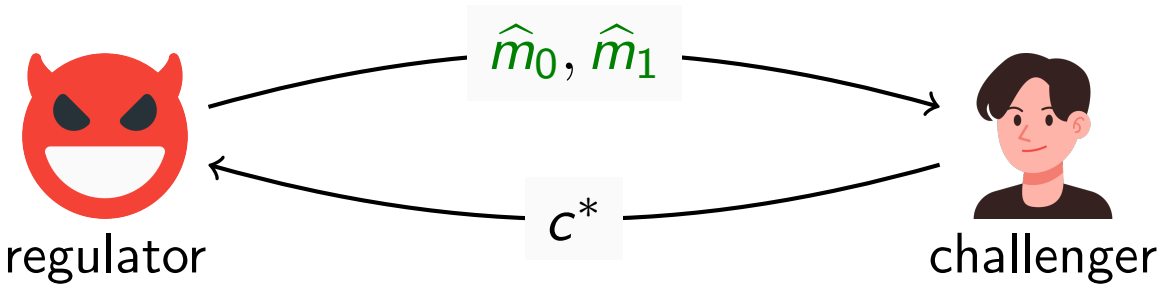
A random function $f \sim \{g : X^k \to X\}$ that outputs one of its input.
Symmetric if for any permutation π we have
$f(x_1, \ldots, x_k) = f(x_{\pi(1)}, \ldots, x_{\pi(k)})$.

Symmetric Choice Function - Useful property

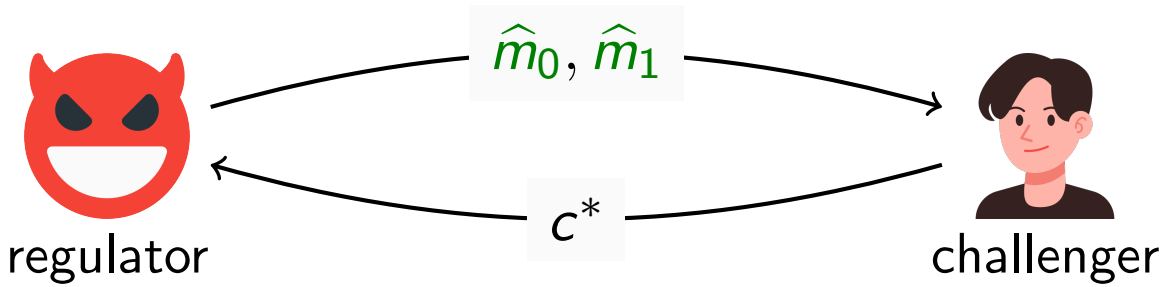
Given $\mathrm{u} \sim U(X^k)$, $\mathrm{v} \sim U(X^{k-1})$ uniformly distributed, let $z = f(\mathrm{u})$. Then

$$\Pr\left[f(z, \mathrm{v}) = z\right] \geq \frac{1}{k} - O\left(\frac{1}{|X|}\right).$$

AsyAE Impossibility - Idea



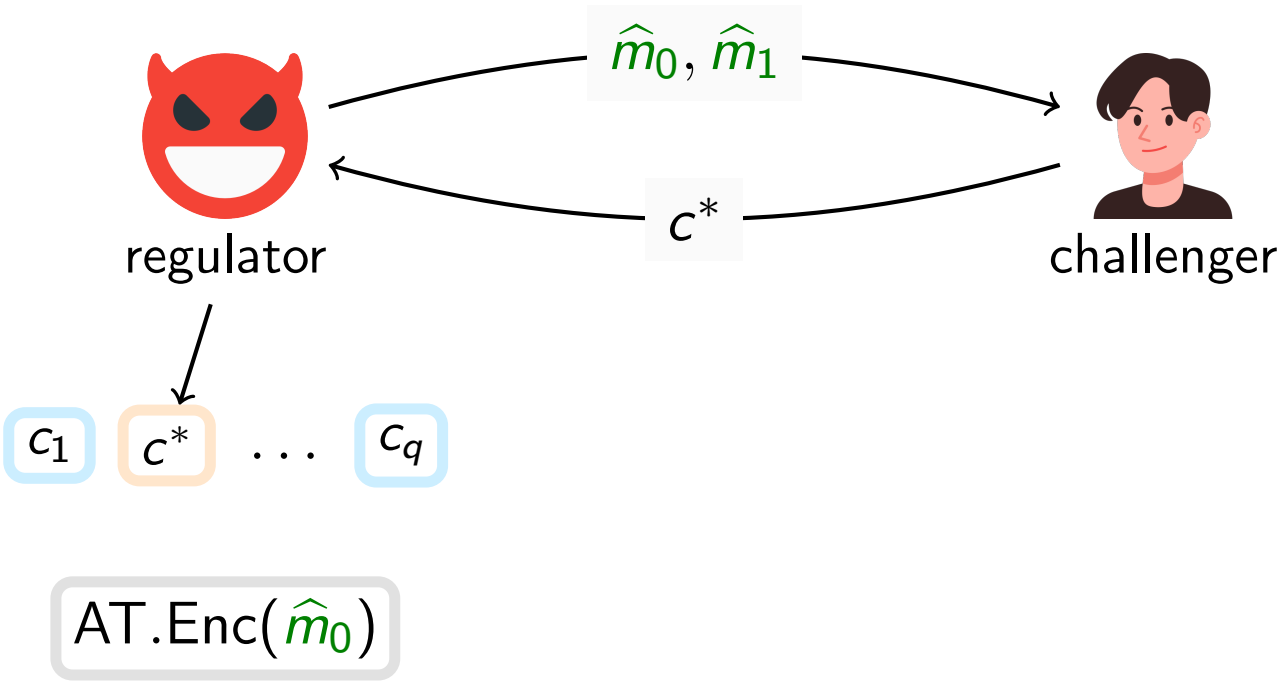
AsyAE Impossibility - Idea



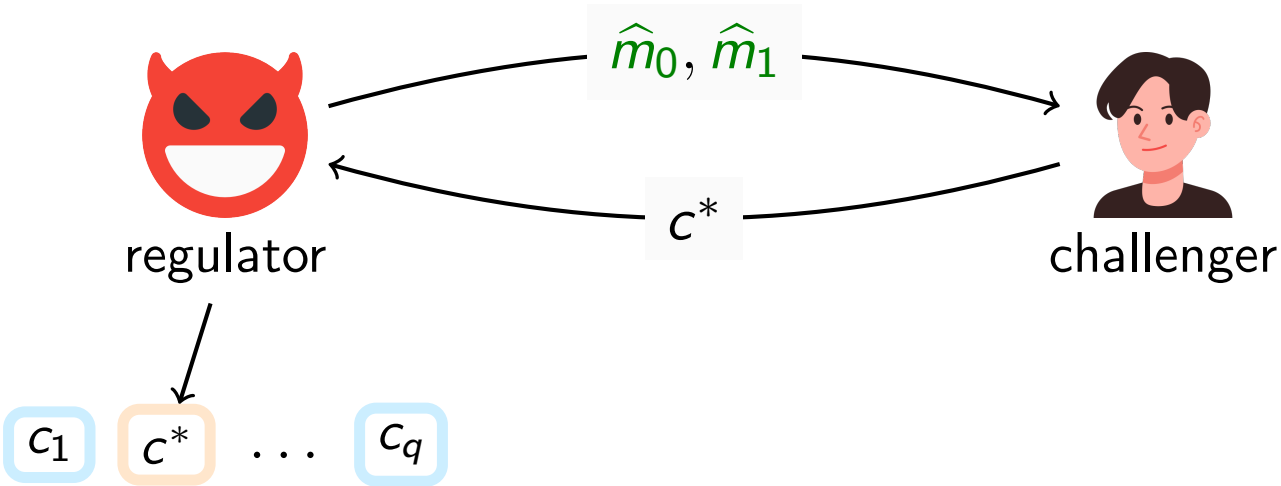
c_1 c_2 ... c_q

$\mathsf{AT.Enc}(\widehat{m}_0)$

AsyAE Impossibility - Idea



AsyAE Impossibility - Idea



$\mathsf{AT.Enc}(\widehat{m}_0) \longrightarrow c'$

$\Pr[c' = c^* \mid b = 0] \approx 1/q$

$\Pr[c' = c_q \mid b = 1] \approx 0$

Dual Construction

⚠* The previous results holds for exponential regular message space

Dual Construction

⚠* The previous results holds for exponential regular message space

What happens when regular message space is poly sized?

Dual Construction

⚠* The previous results holds for exponential regular message space

What happens when regular message space is poly sized?

Black-Box AsyAE with exponential $\widehat{M}$ exists!

Dual Construction

⚠* The previous results holds for exponential regular message space

What happens when regular message space is poly sized?

Black-Box AsyAE with exponential $\widehat{M}$ exists!

Ingredients:

- PKE with pseudorandom ciphertexts Π^{pr}

Dual Construction

$\mathsf{AT.Gen}(\lambda)$:

1. $(\mathsf{pk}, \mathsf{sk}) \leftarrow^{\$} \mathsf{E.Gen}(\lambda)$
2. $(\mathsf{dpk}, \mathsf{dsk}) \leftarrow^{\$} \Pi^{\mathsf{pr}}.\mathsf{Gen}(\lambda)$
2. $\mathsf{apk} \leftarrow \mathsf{pk}, \ \mathsf{ask} \leftarrow \mathsf{sk}$
2. $\mathsf{dk} \leftarrow (\mathsf{dpk}, \mathsf{ask}), \ \mathsf{tk} \leftarrow \mathsf{dsk}$
2. **return** $(\mathsf{apk}, \mathsf{ask}, \mathsf{dk}, \mathsf{tk})$

Dual Construction

$\mathsf{AT.Gen}(\lambda)$:

1. $(\mathsf{pk}, \mathsf{sk}) \leftarrow^{\$} \mathsf{E.Gen}(\lambda)$
2. $(\mathsf{dpk}, \mathsf{dsk}) \leftarrow^{\$} \Pi^{\mathsf{pr}}.\mathsf{Gen}(\lambda)$
2. $\mathsf{apk} \leftarrow \mathsf{pk}, \ \mathsf{ask} \leftarrow \mathsf{sk}$
2. $\mathsf{dk} \leftarrow (\mathsf{dpk}, \mathsf{ask}), \ \mathsf{tk} \leftarrow \mathsf{dsk}$
2. **return** $(\mathsf{apk}, \mathsf{ask}, \mathsf{dk}, \mathsf{tk})$

$\mathsf{AT.Enc}(\mathsf{apk}, \mathsf{dk}, m, \widehat{m})$:

1. Parse dk as $\mathsf{dpk}, \mathsf{dsk}$
1. **do** // Rejection Sampling
1. $\quad c \leftarrow^{\$} \Pi^{\mathsf{pr}}.\mathsf{Enc}(\mathsf{dpk}, \widehat{m})$
2. **while** $m \neq \mathsf{E.Dec}(\mathsf{sk}, c)$
3. **return** c

Dual Construction

$\mathsf{AT.Gen}(\lambda)$:

1. $(\mathsf{pk}, \mathsf{sk}) \leftarrow^{\$} \mathsf{E.Gen}(\lambda)$
2. $(\mathsf{dpk}, \mathsf{dsk}) \leftarrow^{\$} \Pi^{\mathsf{pr}}.\mathsf{Gen}(\lambda)$
2. $\mathsf{apk} \leftarrow \mathsf{pk}, \ \mathsf{ask} \leftarrow \mathsf{sk}$
2. $\mathsf{dk} \leftarrow (\mathsf{dpk}, \mathsf{ask}), \ \mathsf{tk} \leftarrow \mathsf{dsk}$
2. **return** $(\mathsf{apk}, \mathsf{ask}, \mathsf{dk}, \mathsf{tk})$

$\mathsf{AT.Enc}(\mathsf{apk}, \mathsf{dk}, m, \widehat{m})$:

1. Parse dk as $\mathsf{dpk}, \mathsf{dsk}$
1. **do** // Rejection Sampling
1. $\quad c \leftarrow^{\$} \Pi^{\mathsf{pr}}.\mathsf{Enc}(\mathsf{dpk}, \widehat{m})$
2. **while** $m \neq \mathsf{E.Dec}(\mathsf{sk}, c)$
3. **return** c

$\mathsf{AT.Dec}(\mathsf{ask}, \mathsf{tk}, c)$:

1. $\widehat{m} \leftarrow \Pi^{\mathsf{pr}}.\mathsf{Dec}(\mathsf{tk}, c)$
2. **return** $\widehat{m}$

Conclusions and Open Questions

- Black-Box AE is limited to $O(\log(\lambda))$ anamorphic bits of communication $\implies$ RS is optimal
- Black-Box Asymmetric AE is impossibile
- Our results are tight

Open questions

- What properties allows to surpass the lower bound?

Q & A

Thanks for your attention

Any questions?

ia.cr/2024/1098