Generic Anamorphic Encryption, Revisited: New Limitations and Constructions

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

[1]Università di Catania, Italy.

[2]IMDEA Software Institute, Madrid, Spain.

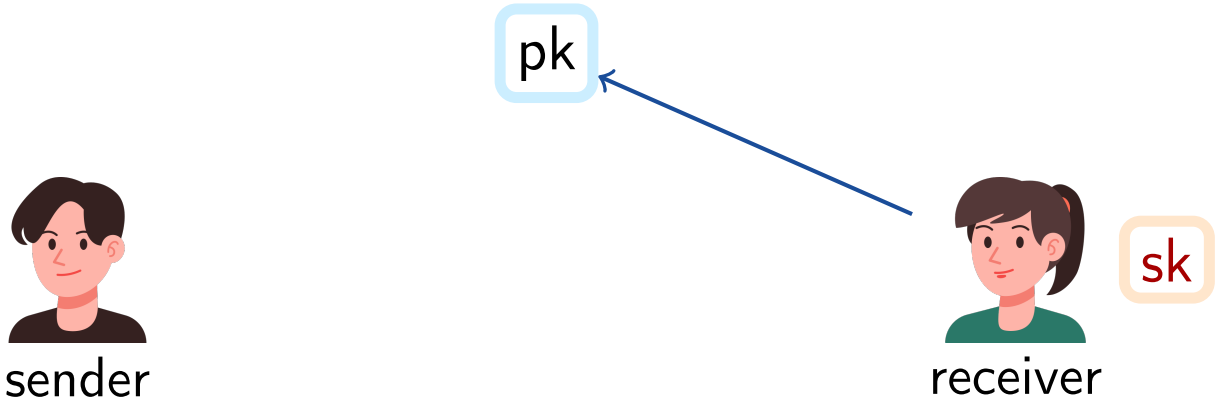
[3]Universidad Politecnica de Madrid, Spain.

Introduction

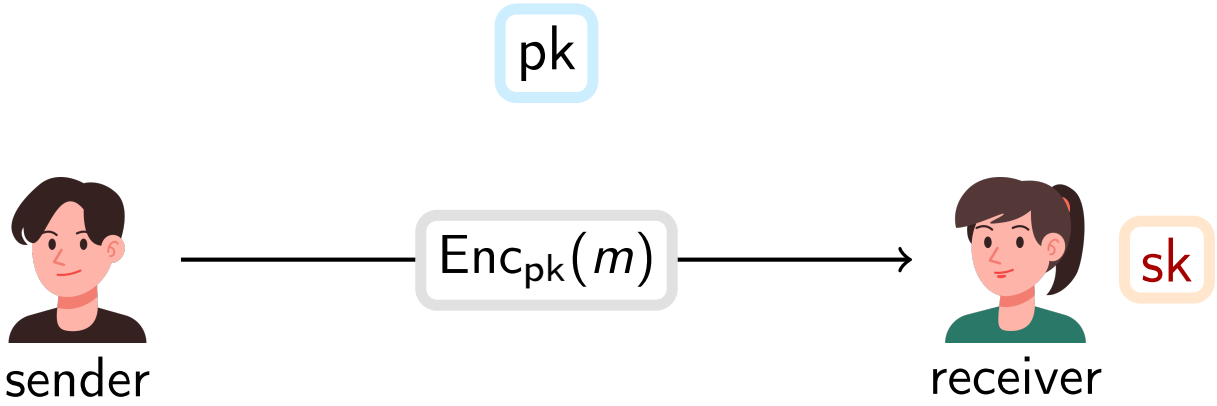
sender

receiver

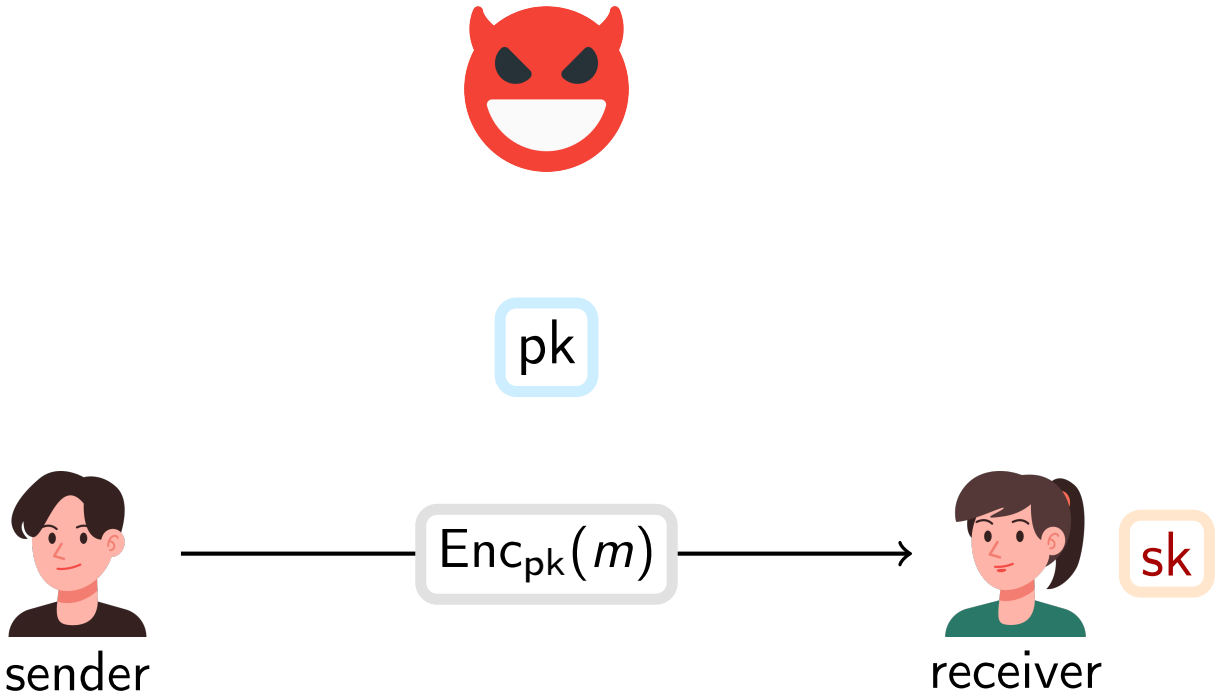
Introduction



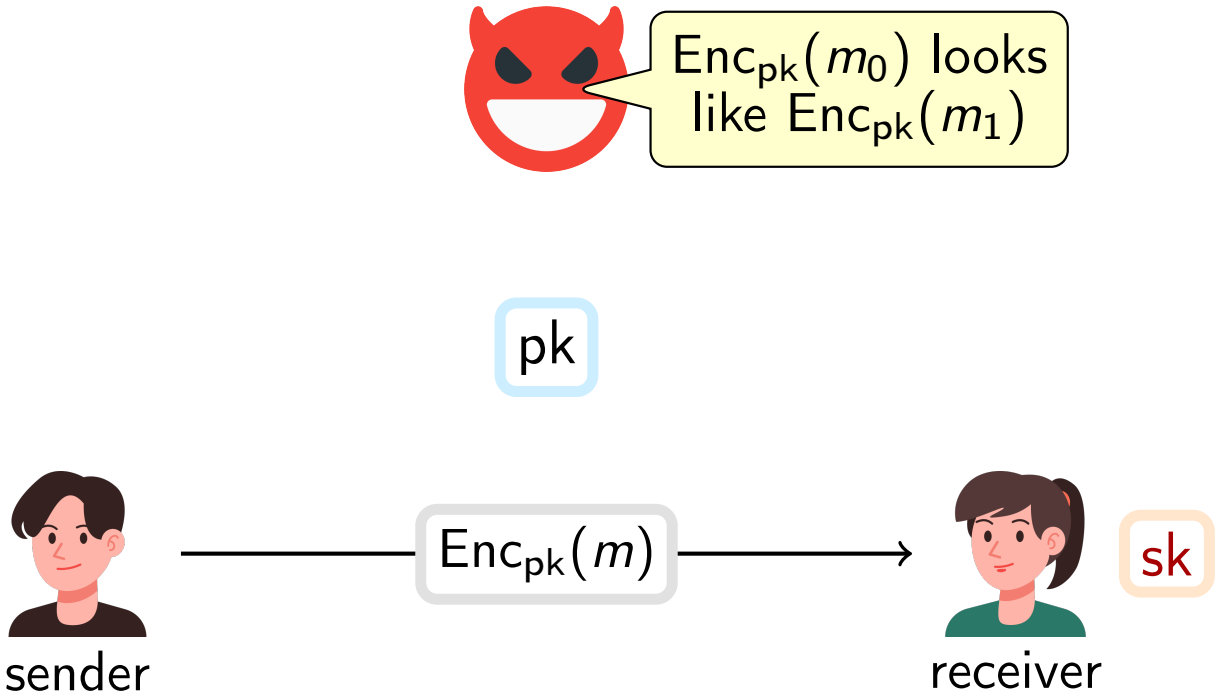
Introduction



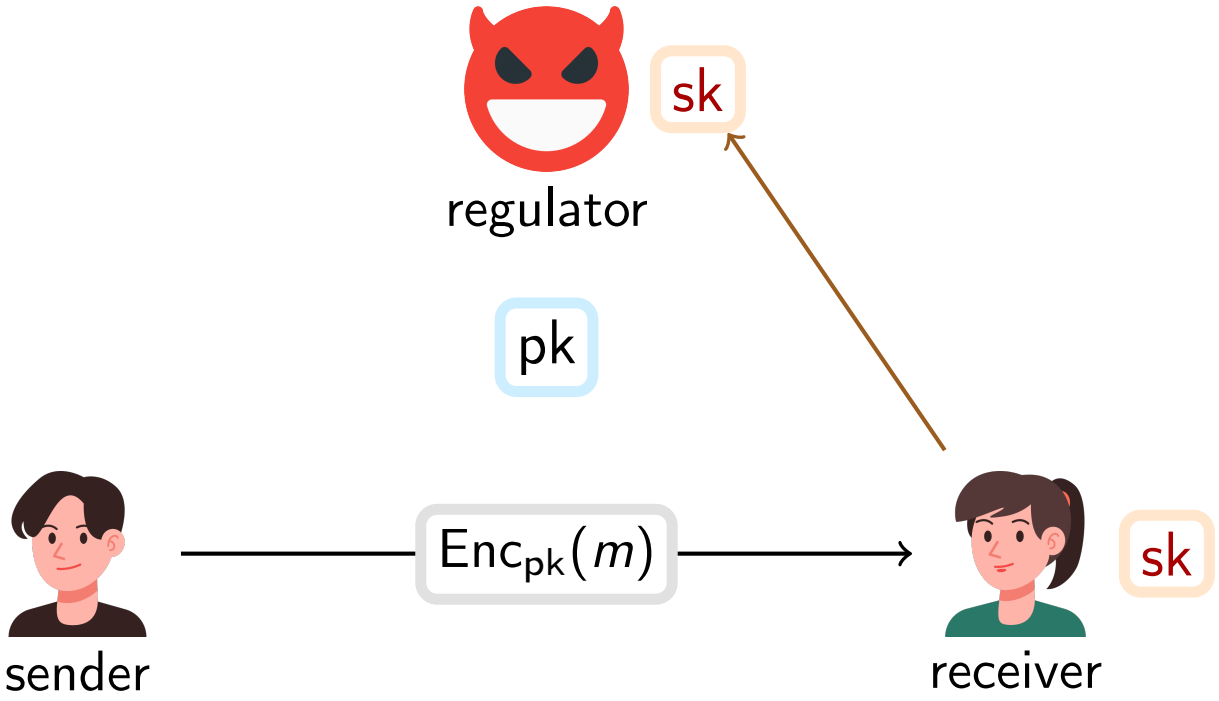
Introduction



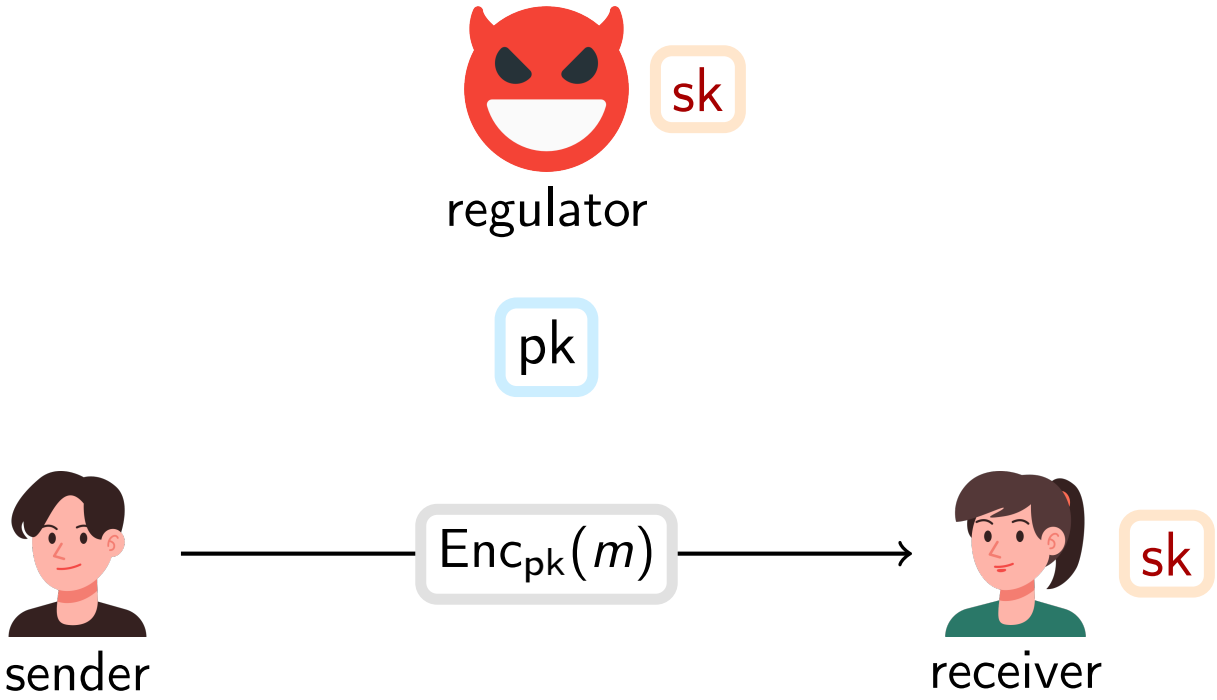
Introduction



Introduction



Introduction



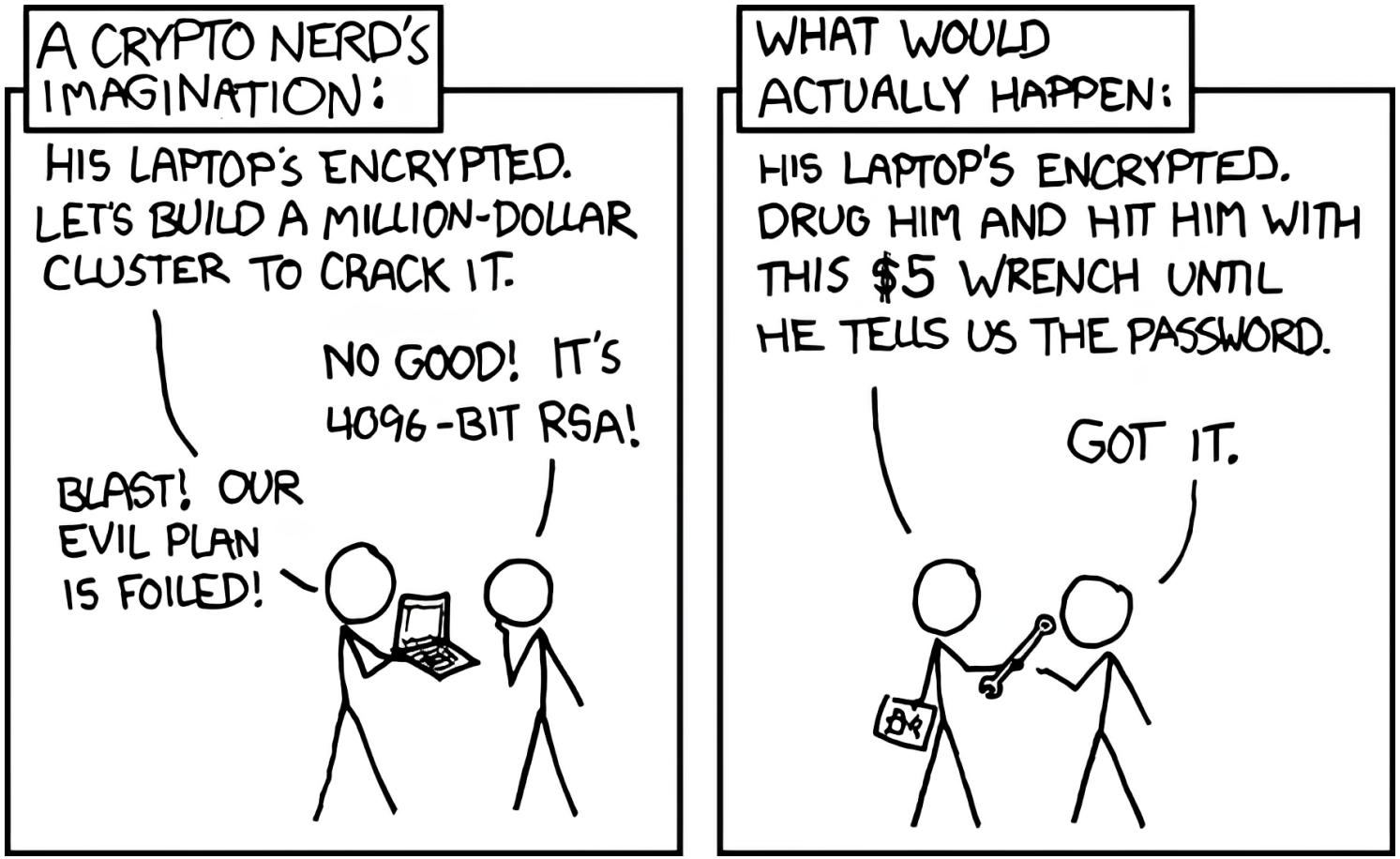
Q. Can we obtain privacy from the regulator?

Implicit assumption

Receiver privacy assumption

Implicit assumption

Receiver privacy assumption



xkcd.com/538/

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

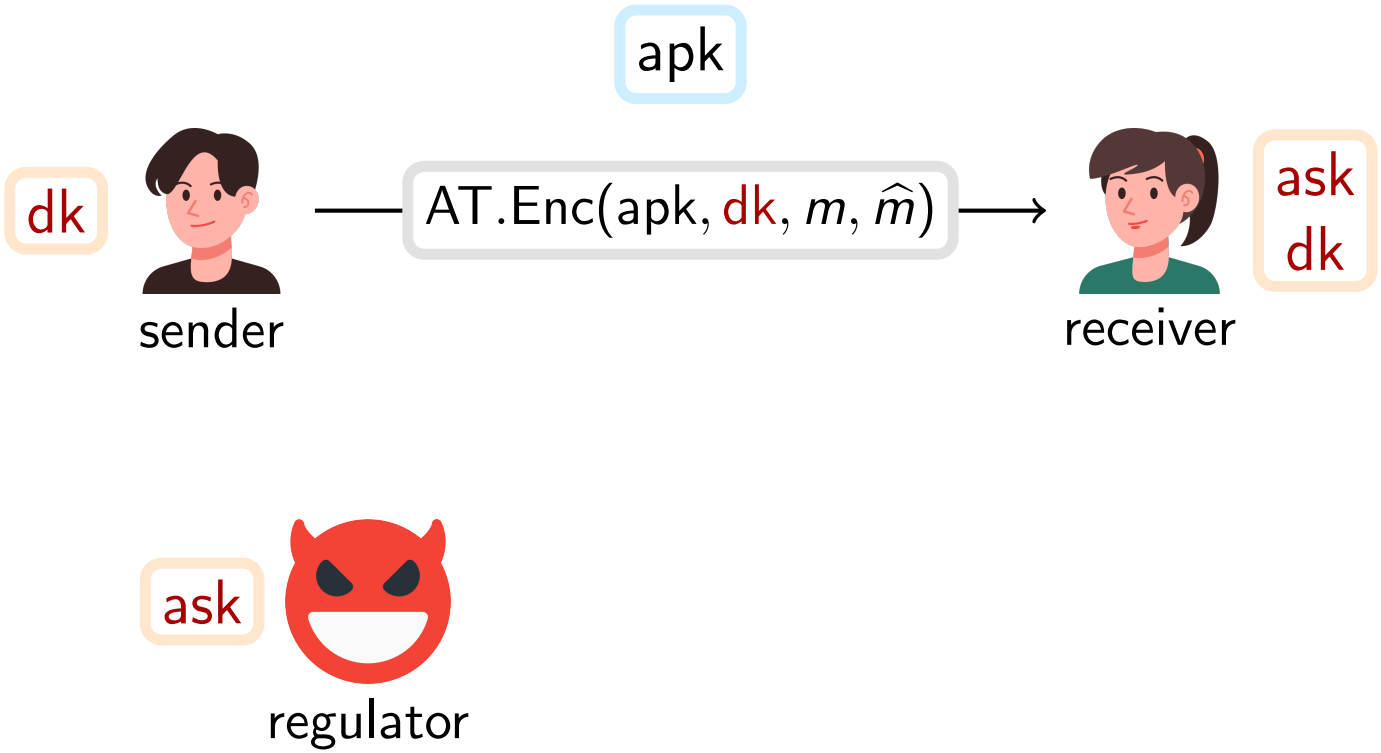
receiver

ask

regulator

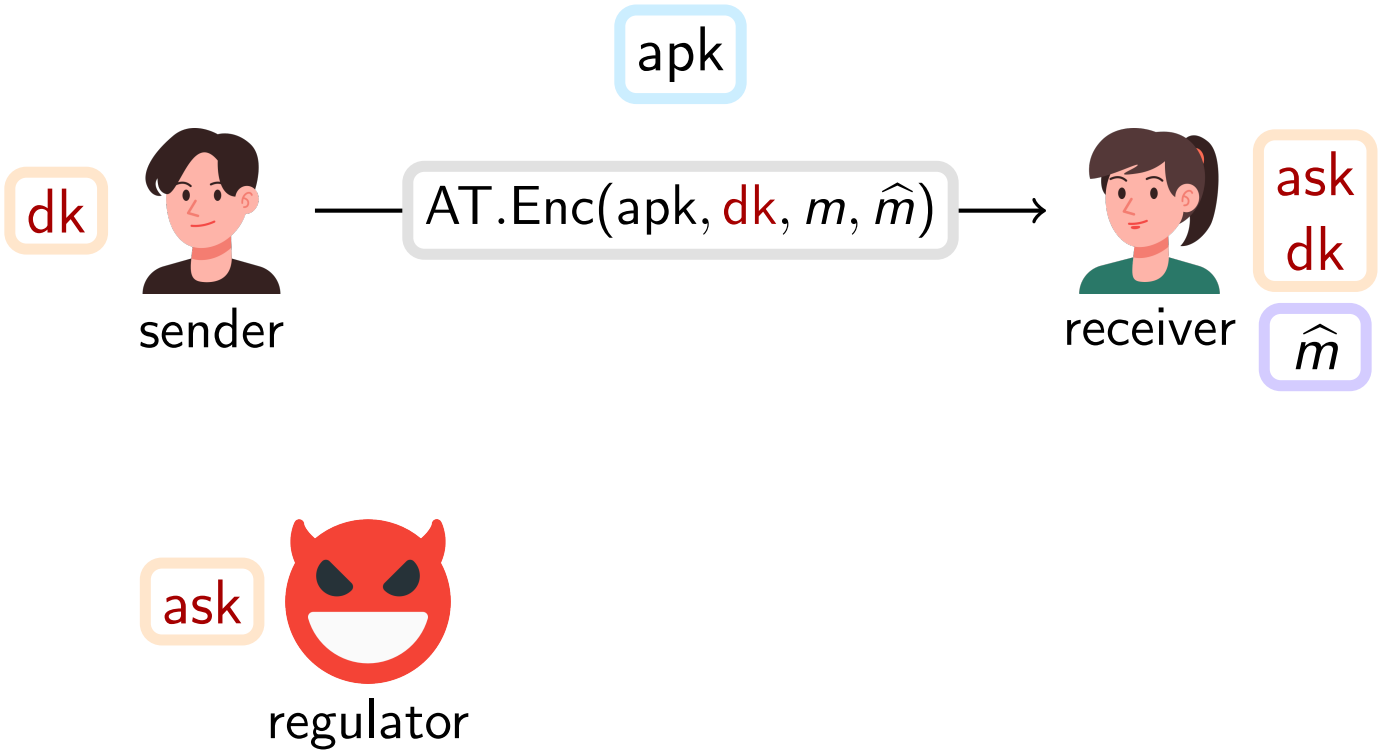
Anamorphic Encryption Definition [PPY22]

AT.Gen AT.Enc AT.Dec



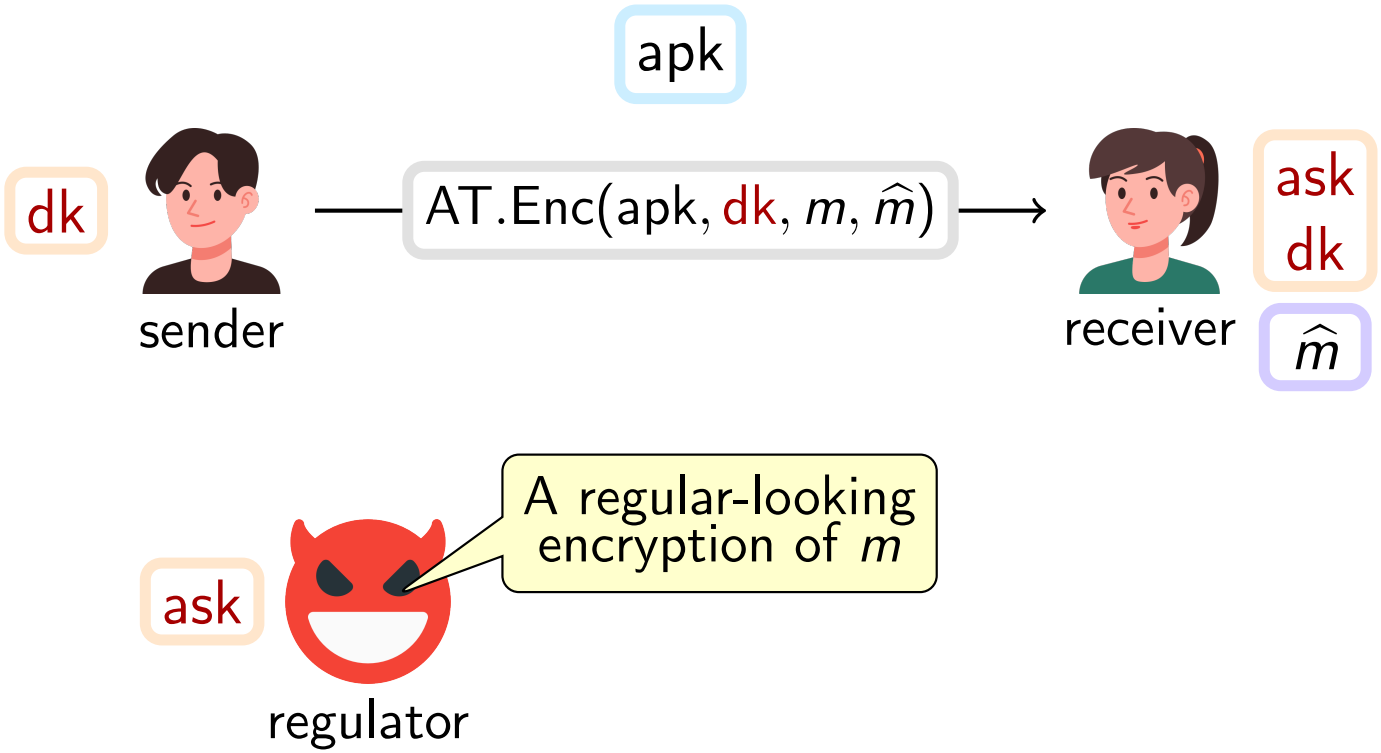
Anamorphic Encryption Definition [PPY22]

AT.Gen AT.Enc AT.Dec



Anamorphic Encryption Definition [PPY22]

AT.Gen AT.Enc AT.Dec

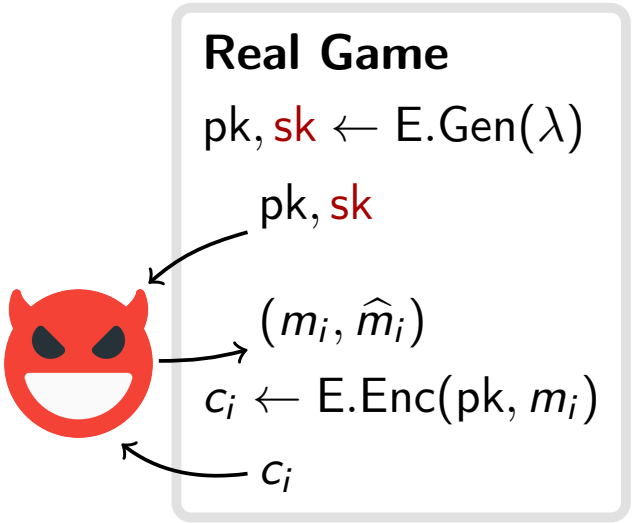


Anamorphic Encryption Definition [PPY22]

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

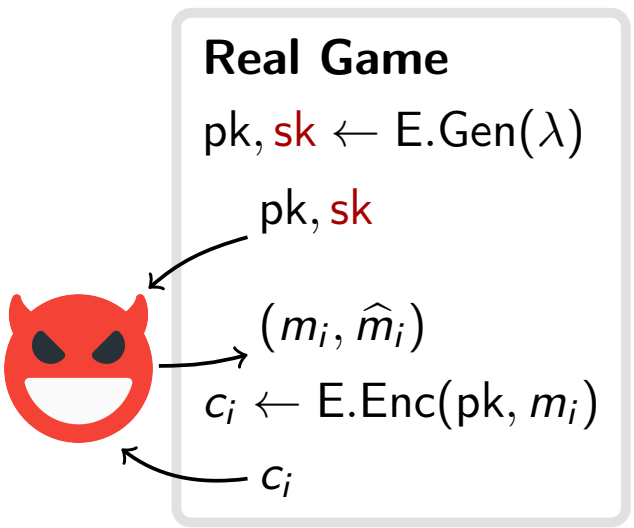
Anamorphic Encryption Definition [PPY22]

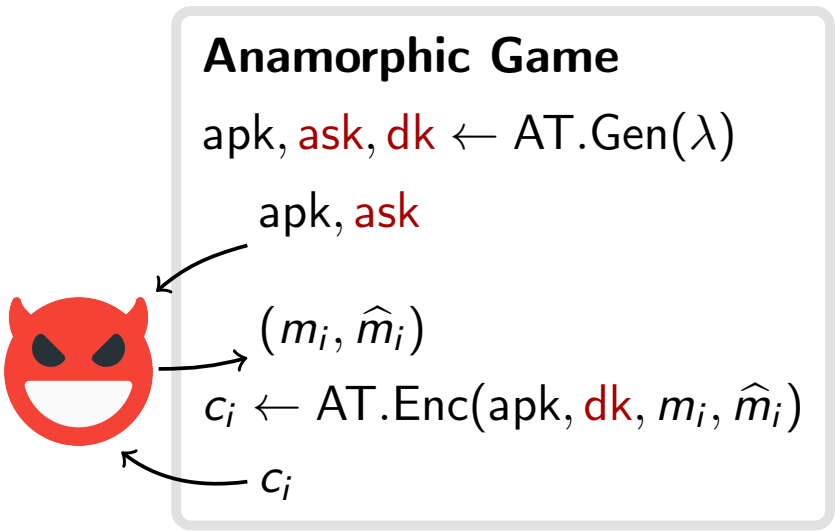
Security of an Anamorphic Triplet (AT.Gen, AT.Enc, AT.Dec) is defined with respect to a PKE (E.Gen, E.Enc, E.Dec).



Anamorphic Encryption Definition [PPY22]

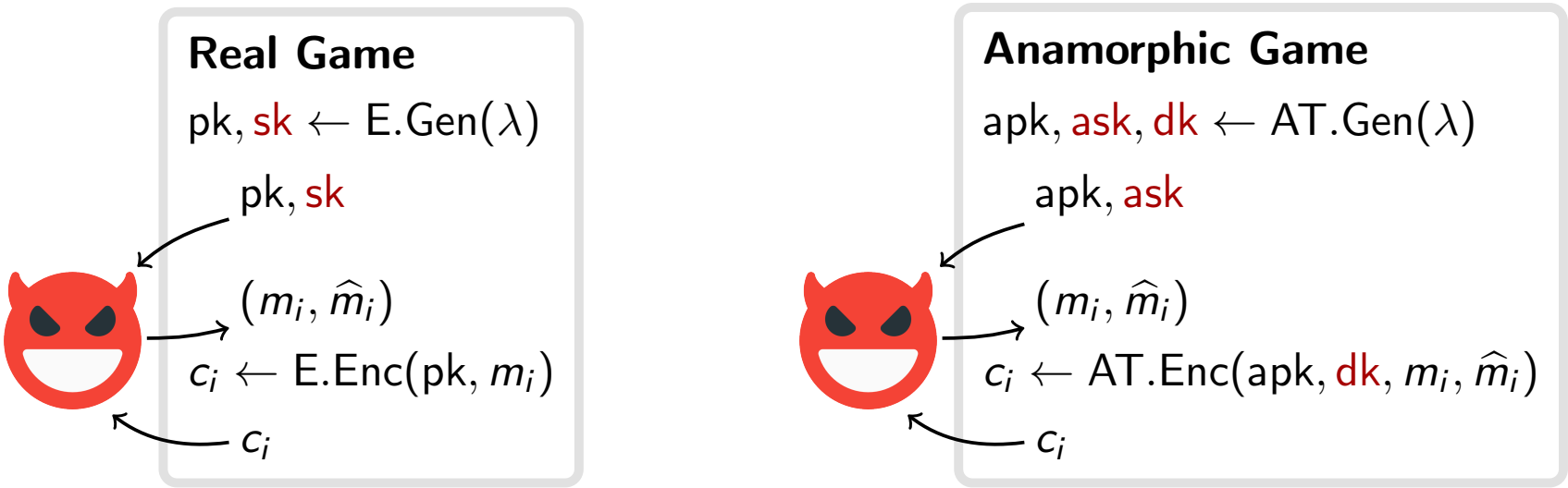
Security of an Anamorphic Triplet (AT.Gen, AT.Enc, AT.Dec) is defined with respect to a PKE (E.Gen, E.Enc, E.Dec).





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).



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

Constructions

Constructions

Specific:

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]

Rejection Sampling Scheme [PPY22]

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

1. $(\mathsf{apk}, \mathsf{ask}) \leftarrow^{\$} \mathsf{E.Gen}(\lambda)$
2. $\mathsf{dk} \leftarrow^{\$} \mathcal{K}$
3. **return** $\mathsf{apk}, \mathsf{ask}, \mathsf{dk}$

Rejection Sampling Scheme [PPY22]

AT.Gen(λ) :

1. $(\mathsf{apk}, \mathsf{ask}) \leftarrow^{\$} \mathsf{E.Gen}(\lambda)$
2. $\mathsf{dk} \leftarrow^{\$} \mathcal{K}$
3. **return** $\mathsf{apk}, \mathsf{ask}, \mathsf{dk}$

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

1. $c \leftarrow \mathsf{E.Enc}(\mathsf{pk}, m)$
2. **if** $\mathsf{PRF}(\mathsf{dk}, c) \neq \widehat{m}$: **retry**
3. **else**: **return** c

Rejection Sampling Scheme [PPY22]

AT.Gen(λ) :

1. $(\mathsf{apk}, \mathsf{ask}) \leftarrow^{\$} \mathsf{E.Gen}(\lambda)$
2. $\mathsf{dk} \leftarrow^{\$} \mathcal{K}$
3. **return** $\mathsf{apk}, \mathsf{ask}, \mathsf{dk}$

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

1. $c \leftarrow \mathsf{E.Enc}(\mathsf{pk}, m)$
2. **if** $\mathsf{PRF}(\mathsf{dk}, c) \neq \widehat{m}$: **retry**
3. **else**: **return** c

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

1. $\widehat{m} \leftarrow \mathsf{PRF}(\mathsf{dk}, c)$
2. **return** $\widehat{m}$

Rejection Sampling Scheme [PPY22]

AT.Gen(λ) :

1. $(\mathsf{apk}, \mathsf{ask}) \leftarrow^{\$} \mathsf{E.Gen}(\lambda)$
2. $\mathsf{dk} \leftarrow^{\$} \mathcal{K}$
3. **return** $\mathsf{apk}, \mathsf{ask}, \mathsf{dk}$

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

1. $c \leftarrow \mathsf{E.Enc}(\mathsf{pk}, m)$
2. **if** $\mathsf{PRF}(\mathsf{dk}, c) \neq \widehat{m}$: **retry**
3. **else**: **return** c

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

1. $\widehat{m} \leftarrow \mathsf{PRF}(\mathsf{dk}, c)$
2. **return** $\widehat{m}$

- Only supports $O(\log \lambda)$ bits long messages.

Rejection Sampling Scheme [PPY22]

AT.Gen(λ) :

1. $(\mathsf{apk}, \mathsf{ask}) \leftarrow^{\$} \mathsf{E.Gen}(\lambda)$
2. $\mathsf{dk} \leftarrow^{\$} \mathcal{K}$
3. **return** $\mathsf{apk}, \mathsf{ask}, \mathsf{dk}$

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

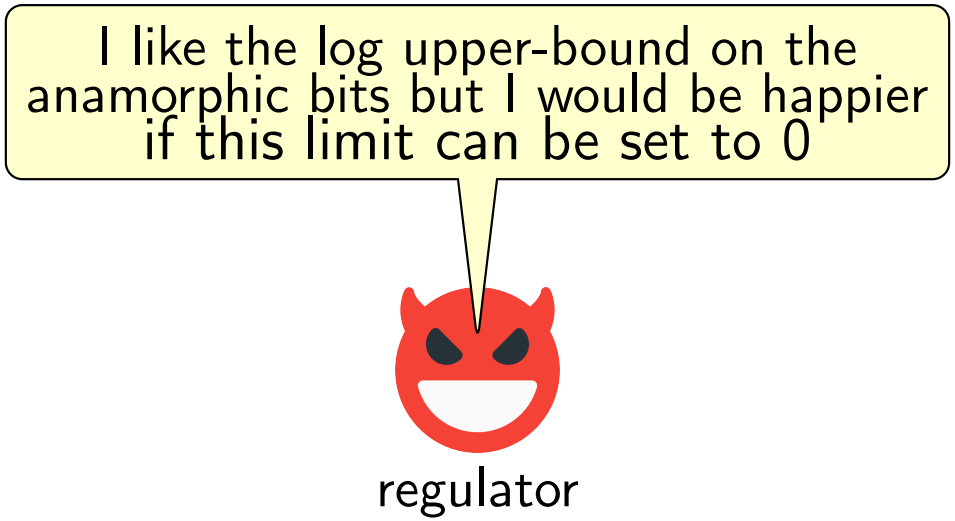
1. $c \leftarrow \mathsf{E.Enc}(\mathsf{pk}, m)$
2. **if** $\mathsf{PRF}(\mathsf{dk}, c) \neq \widehat{m}$: **retry**
3. **else**: **return** c

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

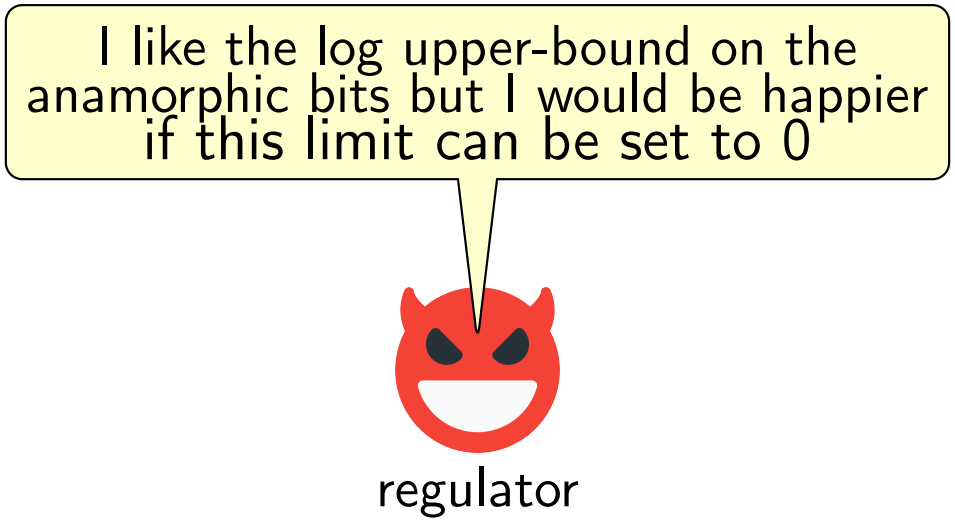
1. $\widehat{m} \leftarrow \mathsf{PRF}(\mathsf{dk}, c)$
2. **return** $\widehat{m}$

- Supports $O(\log \lambda)$ bits long messages. [CGM24b]

Question


I like the log upper-bound on the anamorphic bits but I would be happier if this limit can be set to 0
regulator

Question



Q. There exists an Anamorphic Triplet for any PKE?

Weak PKE - example

Weak PKE - example

- Injective OWF F
- A set B s.t. $|B| = \text{poly}(\lambda)$ disjoint from C

Weak PKE - example

$\mathsf{E.Gen}^*(\lambda)$:

1. $\mathsf{pk}, \mathsf{sk} \leftarrow^{\$} \mathsf{E.Gen}(\lambda)$
2. $m^* \leftarrow^{\$} M,\ y^* \leftarrow F(m^*)$
3. $\mathsf{pk}^* \leftarrow (\mathsf{pk}, y^*),\ \mathsf{sk}^* \leftarrow (\mathsf{sk}, m^*)$
4. **return** $(\mathsf{pk}^*, \mathsf{sk}^*)$

Weak PKE - example

$\mathsf{E.Gen}^*(\lambda)$:

1. $\mathsf{pk}, \mathsf{sk} \leftarrow^{\$} \mathsf{E.Gen}(\lambda)$
2. $m^* \leftarrow^{\$} M,\ y^* \leftarrow F(m^*)$
3. $\mathsf{pk}^* \leftarrow (\mathsf{pk}, y^*),\ \mathsf{sk}^* \leftarrow (\mathsf{sk}, m^*)$
4. **return** $(\mathsf{pk}^*, \mathsf{sk}^*)$

$\mathsf{E.Enc}^*(\mathsf{pk}^*, m)$:

1. Parse $\mathsf{pk}^* = (\mathsf{pk}, y^*)$
2. **if** $F(m) = y^*$:
3. **return** $c \leftarrow^{\$} B$
4. **else**:
5. **return** $c \leftarrow^{\$} \mathsf{E.Enc}(\mathsf{pk}, m)$

Weak PKE - example

$\mathsf{E.Gen}^*(\lambda)$:

1. $\mathsf{pk}, \mathsf{sk} \leftarrow^{\$} \mathsf{E.Gen}(\lambda)$
2. $m^* \leftarrow^{\$} M,\ y^* \leftarrow F(m^*)$
3. $\mathsf{pk}^* \leftarrow (\mathsf{pk}, y^*),\ \mathsf{sk}^* \leftarrow (\mathsf{sk}, m^*)$
4. **return** $(\mathsf{pk}^*, \mathsf{sk}^*)$

$\mathsf{E.Enc}^*(\mathsf{pk}^*, m)$:

1. Parse $\mathsf{pk}^* = (\mathsf{pk}, y^*)$
2. **if** $F(m) = y^*$:
3. **return** $c \leftarrow^{\$} B$
4. **else**:
5. **return** $c \leftarrow^{\$} \mathsf{E.Enc}(\mathsf{pk}, m)$

$\mathsf{E.Dec}^*(\mathsf{sk}^*, c)$:

1. Parse $\mathsf{sk}^* = (\mathsf{sk}, m^*)$
2. **if** $c \in B$: **return** m^*
3. **else**: **return** $\mathsf{E.Dec}(\mathsf{sk}, c)$

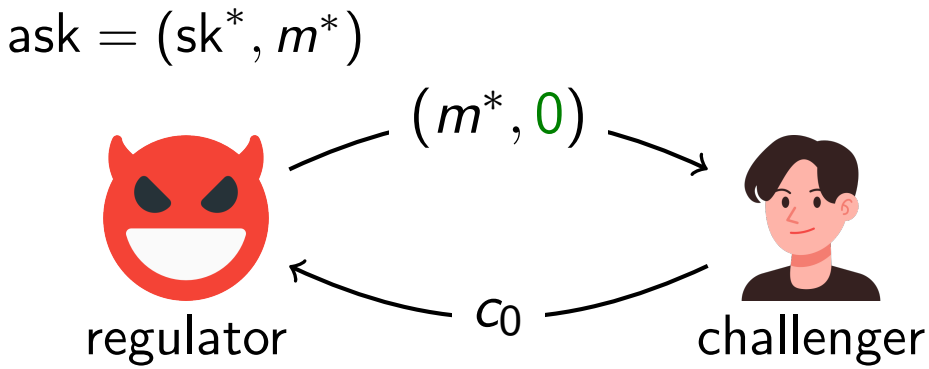
Weak PKE - example

$$\mathsf{ask} = (\mathsf{sk}^*, m^*)$$

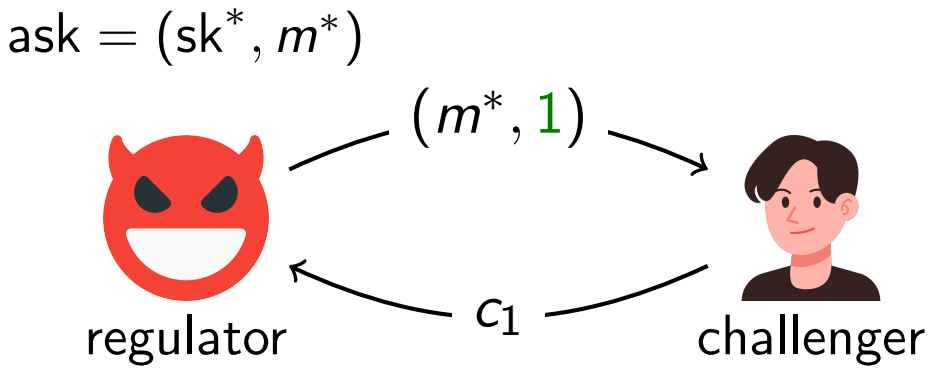
regulator

challenger

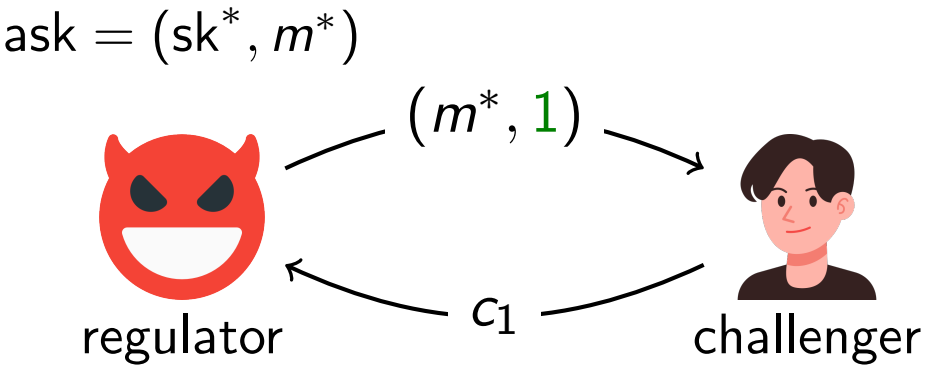
Weak PKE - example



Weak PKE - example

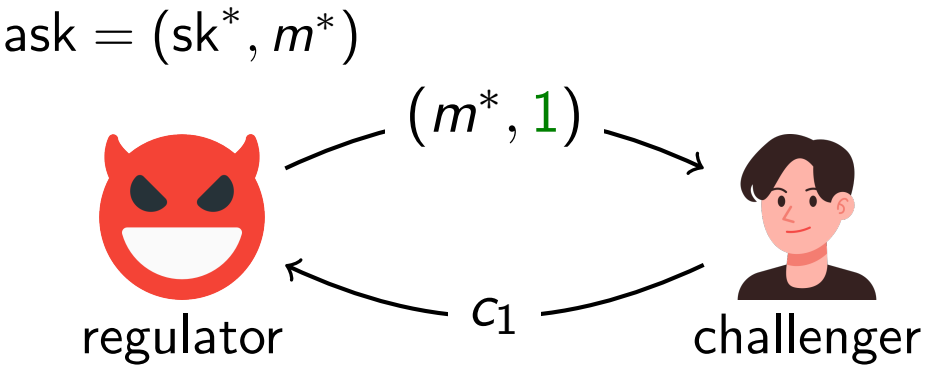


Weak PKE - example



return $c_0 == c_1$

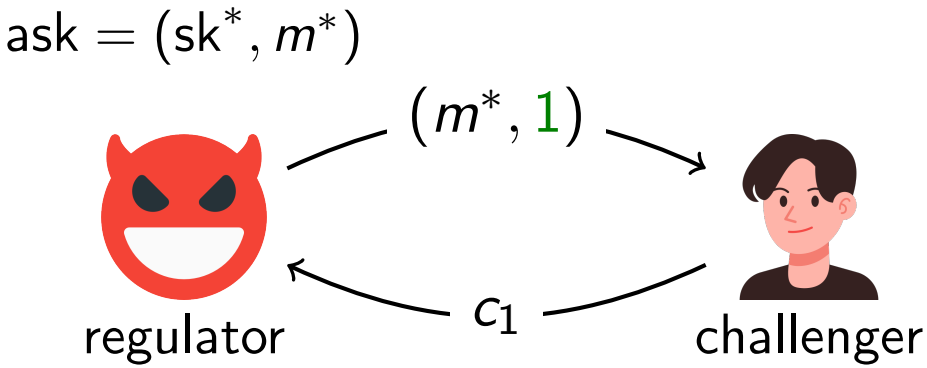
Weak PKE - example



return $c_0 == c_1$

$$\Pr[c_0 = c_1 \mid \text{Real Game}] = 1/|B|$$

Weak PKE - example



return $c_0 == c_1$

$$\Pr[c_0 = c_1 \mid \text{Real Game}] = 1/|B|$$

$$\Pr[c_0 = c_1 \mid \text{Anamorphic Game}] = 1/|B|(1/2 + \text{negl}(\lambda))$$

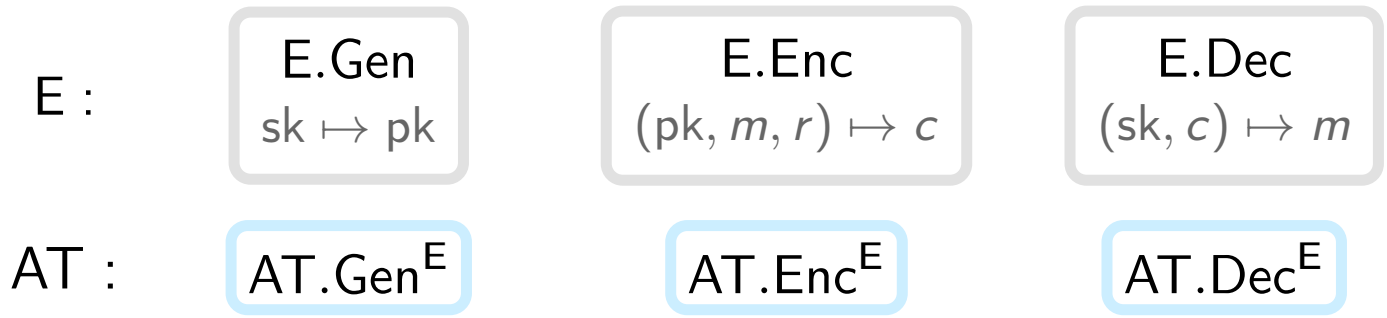
Black-Box Anamorphic Encryption

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

Black-Box Anamorphic Encryption

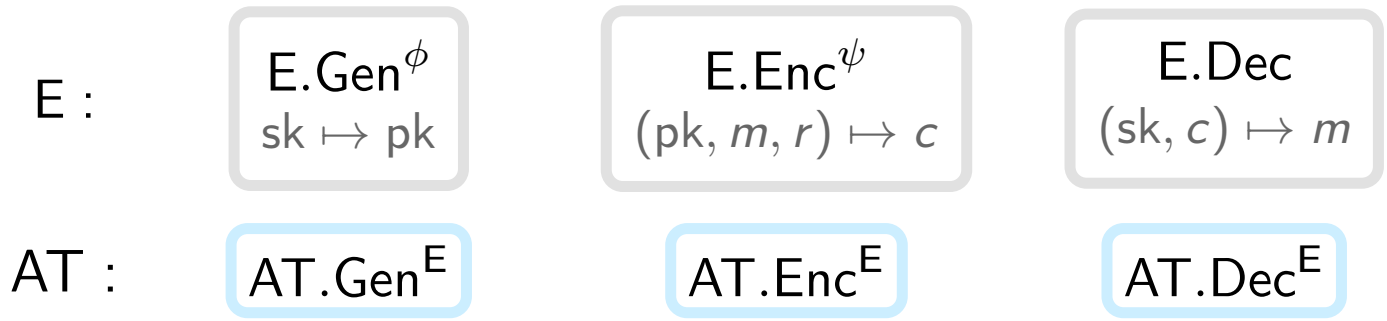
E :	E.Gen $\mathsf{sk} \mapsto \mathsf{pk}$	E.Enc $(\mathsf{pk}, m, r) \mapsto c$	E.Dec $(\mathsf{sk}, c) \mapsto m$
AT :	$\mathsf{AT.Gen}^{\mathsf{E}}$	$\mathsf{AT.Enc}^{\mathsf{E}}$	$\mathsf{AT.Dec}^{\mathsf{E}}$

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.

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

Weak Messages

A message m^* is a weak one if:

Weak Messages

A message m^* is a weak one if:

- Has only poly many valid ciphertexts

Weak Messages

A message m^* is a weak one if:

- Has only poly many valid ciphertexts
- $m^* \approx m$ for a random m

Weak Messages

A message m^* is a weak one if:

- Has only poly many valid ciphertexts
- $m^* \approx m$ for a random m
- m^* is hard to find given only pk

Weak PKE

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

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

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

Weak PKE

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

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

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

$\mathsf{E.Find}$
$(\mathsf{sk}, i) \mapsto m_i^*(\mathsf{sk})$

Weak PKE

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

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

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

$\mathsf{E.Find}$
$(\mathsf{sk}, i) \mapsto m_i^*(\mathsf{sk})$

Ideal PKE: Take E.Gen, E.Enc and m_i^* as truly random functions.

Weak PKE

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

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

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

$\mathsf{E.Find}$
$(\mathsf{sk}, i) \mapsto m_i^*(\mathsf{sk})$

Ideal PKE: Take E.Gen, E.Enc and m_i^* as truly random functions.

τ is a randomness biasing function.
Acts as identity on *good* messages, compresses on *weak* messages.

IND-CPA proof idea

- sk is random $\implies$ sk is hard to find

IND-CPA proof idea

- sk is random $\implies$ sk is hard to find
- if sk is unknown then $m_i^*(\mathsf{sk})$ is random $\implies$ m_b is not weak

IND-CPA proof idea

- sk is random $\implies$ sk is hard to find
- if sk is unknown then $m_i^*(\mathsf{sk})$ is random $\implies$ m_b is not weak
- if c^* is never decrypted and m_b is not weak $\implies$ $\mathcal{A}$ cannot query E.Enc with the same randomness as used to generate the challenge ciphertext

Weak PKE - adversary

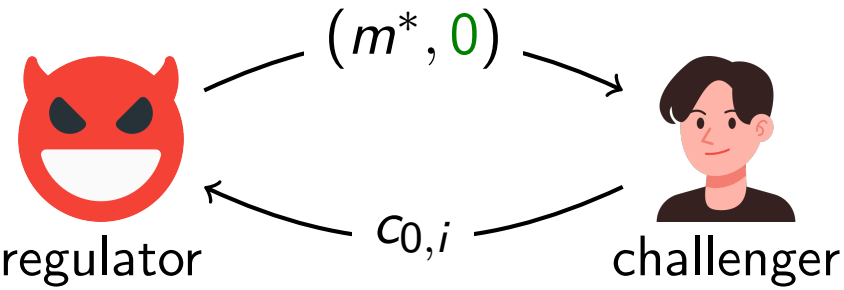
$m^* \leftarrow \mathsf{E.Find}(\mathsf{sk}, \log \nu)$

regulator

challenger

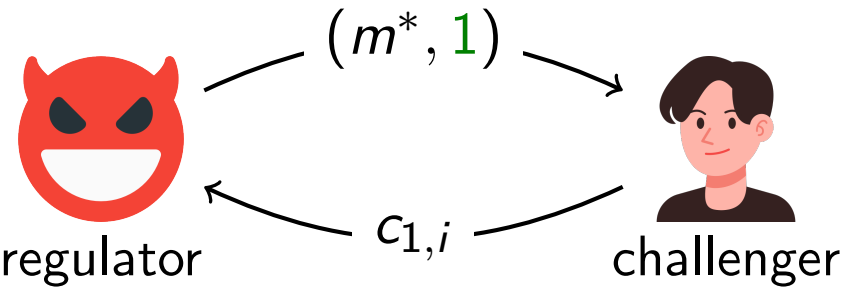
Weak PKE - adversary

$m^* \leftarrow \mathsf{E.Find}(\mathsf{sk}, \log \nu)$



Weak PKE - adversary

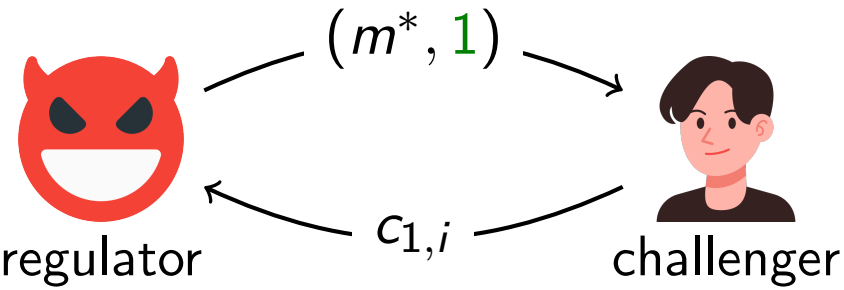
$m^* \leftarrow \mathsf{E.Find}(\mathsf{sk}, \log \nu)$



return 0 **if** $\nexists i, j$ s.t. $c_{0,i} = c_{1,j}$

Weak PKE - adversary

$m^* \leftarrow \mathsf{E.Find}(\mathsf{sk}, \log \nu)$

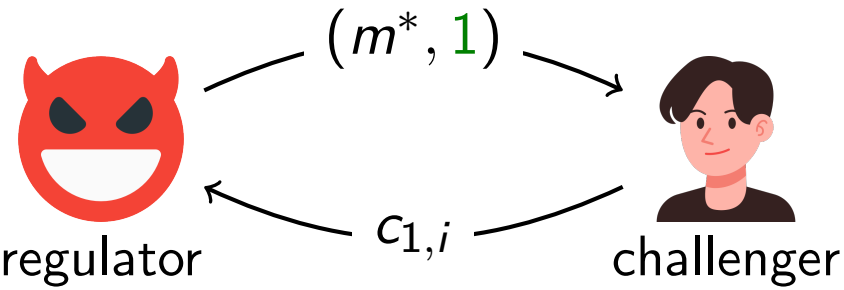


return 0 **if** $\nexists i, j$ s.t. $c_{0,i} = c_{1,j}$

$$\Pr[c_0 = c_1 \mid \text{Real Game}] \geq (1 - e^{-1})/2$$

Weak PKE - adversary

$m^* \leftarrow \mathsf{E.Find}(\mathsf{sk}, \log \nu)$



return 0 **if** $\nexists i, j$ s.t. $c_{0,i} = c_{1,j}$

$$\Pr[c_0 = c_1 \mid \text{Real Game}] \geq (1 - e^{-1})/2$$

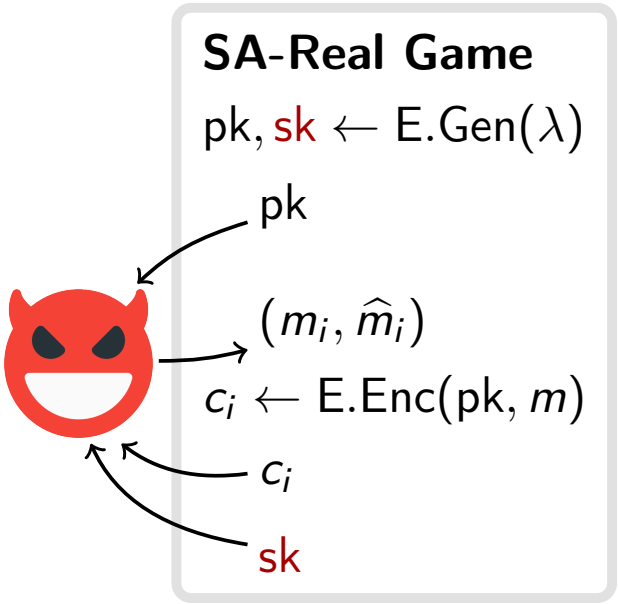
$$\Pr[c_0 = c_1 \mid \text{Anamorphic Game}] \leq 1/(\lambda\sqrt{2})$$

Positive results

Semi-Adaptive security.

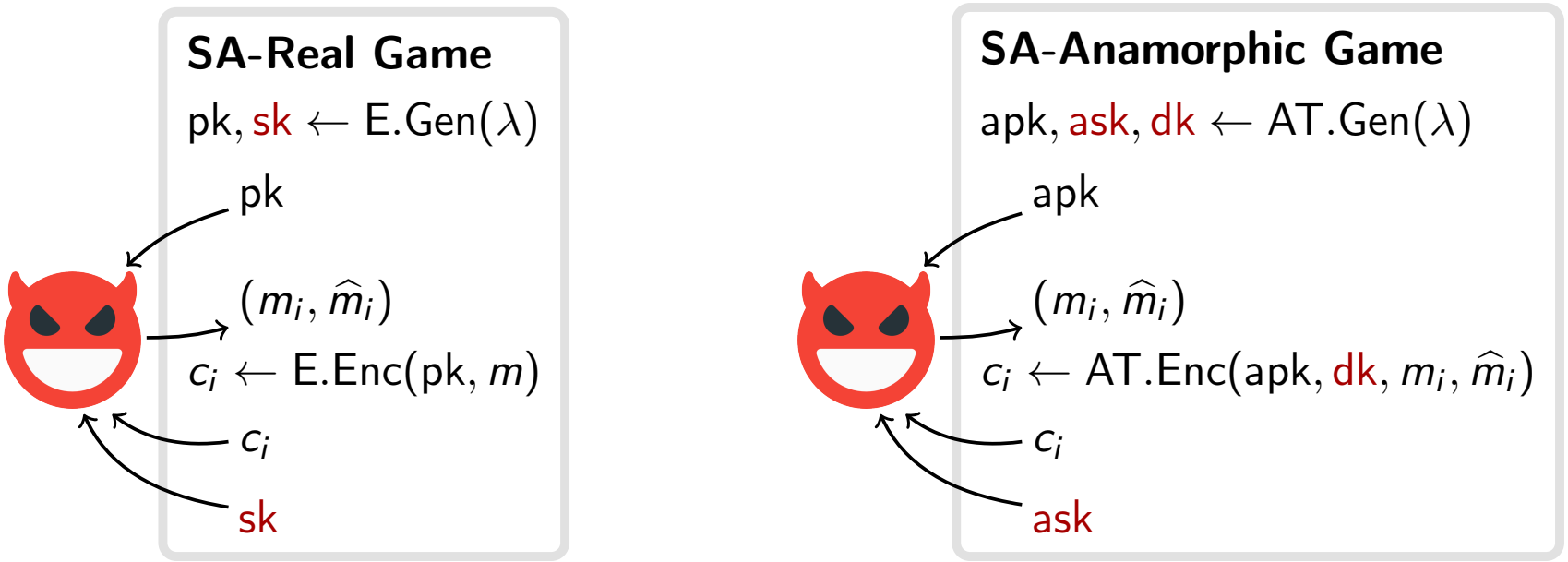
Positive results

Semi-Adaptive security.



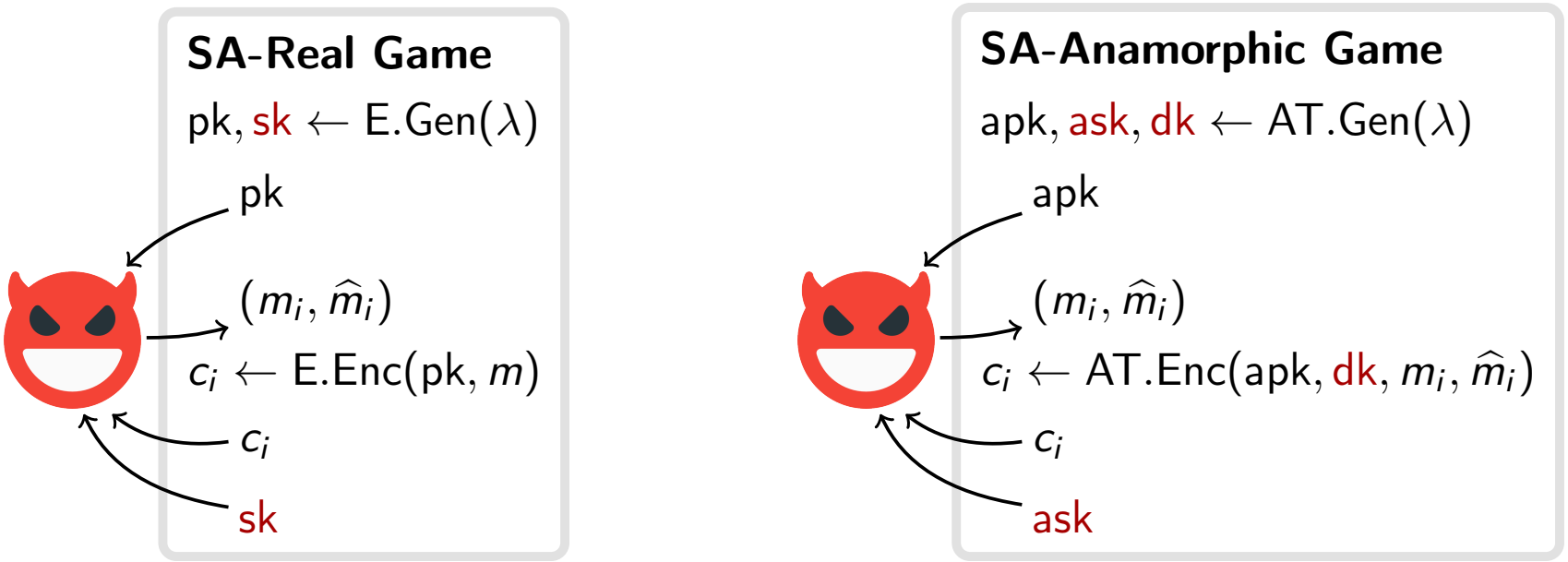
Positive results

Semi-Adaptive security.



Positive results

Semi-Adaptive security.



SA-Real Game $\overset{c}{\approx}$ SA-Anamorphic Game

Limits of Semi-Adaptive AE

Results from [CGM24b] are "imported"

Limits of Semi-Adaptive AE

Results from [CGM24b] are "imported"

- Any black-box SA Anamorphic Triplet can transmit at most $O(\log \lambda)$ anamorphic bits

Limits of Semi-Adaptive AE

Results from [CGM24b] are "imported"

- Any black-box SA Anamorphic Triplet can transmit at most $O(\log \lambda)$ anamorphic bits
- Black-box Asymmetric SA-AE is impossible

Rejection Sampling Scheme [PPY22]

AT.Gen(λ) :

1. $(\mathsf{apk}, \mathsf{ask}) \leftarrow^{\$} \mathsf{E.Gen}(\lambda)$
2. $\mathsf{dk} \leftarrow^{\$} \mathcal{K}$
3. **return** $\mathsf{apk}, \mathsf{ask}, \mathsf{dk}$

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

1. $c \leftarrow \mathsf{E.Enc}(\mathsf{pk}, m)$
2. **if** $\mathsf{PRF}(\mathsf{dk}, c) \neq \widehat{m}$: **retry**
3. **else**: **return** c

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

1. $\widehat{m} \leftarrow \mathsf{PRF}(\mathsf{dk}, c)$
2. **return** $\widehat{m}$

Rejection Sampling Scheme [PPY22]

AT.Gen(λ) :

1. $(\mathsf{apk}, \mathsf{ask}) \leftarrow^{\$} \mathsf{E.Gen}(\lambda)$
2. $\mathsf{dk} \leftarrow^{\$} \mathcal{K}$
3. **return** $\mathsf{apk}, \mathsf{ask}, \mathsf{dk}$

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

1. $c \leftarrow \mathsf{E.Enc}(\mathsf{pk}, m)$
2. **if** $\mathsf{PRF}(\mathsf{dk}, c) \neq \widehat{m}$: **retry**
3. **else**: **return** c

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

1. $\widehat{m} \leftarrow \mathsf{PRF}(\mathsf{dk}, c)$
2. **return** $\widehat{m}$

✅ Works **for almost* any** secure and correct PKE!

⚠* If for all m, $\mathrm{H}_\infty(\mathsf{E.Enc}(\mathsf{pk}, m)) = \omega(\log \lambda)$

Rejection Sampling Scheme [PPY22]

AT.Gen(λ) :

1. $(\mathsf{apk}, \mathsf{ask}) \leftarrow^{\$} \mathsf{E.Gen}(\lambda)$
2. $\mathsf{dk} \leftarrow^{\$} \mathcal{K}$
3. **return** $\mathsf{apk}, \mathsf{ask}, \mathsf{dk}$

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

1. $c \leftarrow \mathsf{E.Enc}(\mathsf{pk}, m)$
2. **if** $\mathsf{PRF}(\mathsf{dk}, c) \neq \widehat{m}$: **retry**
3. **else**: **return** c

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

1. $\widehat{m} \leftarrow \mathsf{PRF}(\mathsf{dk}, c)$
2. **return** $\widehat{m}$

- Works **for almost* any** secure and correct PKE!
- * If for all m, $\mathrm{H}_\infty(\mathsf{E.Enc}(\mathsf{pk}, m)) = \omega(\log \lambda)$
- It is Semi-Adaptive for any secure and correct PKE!

Rejection Sampling Scheme [PPY22]

AT.Gen(λ) :

1. $(\mathsf{apk}, \mathsf{ask}) \leftarrow^{\$} \mathsf{E.Gen}(\lambda)$
2. $\mathsf{dk} \leftarrow^{\$} \mathcal{K}$
3. **return** $\mathsf{apk}, \mathsf{ask}, \mathsf{dk}$

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

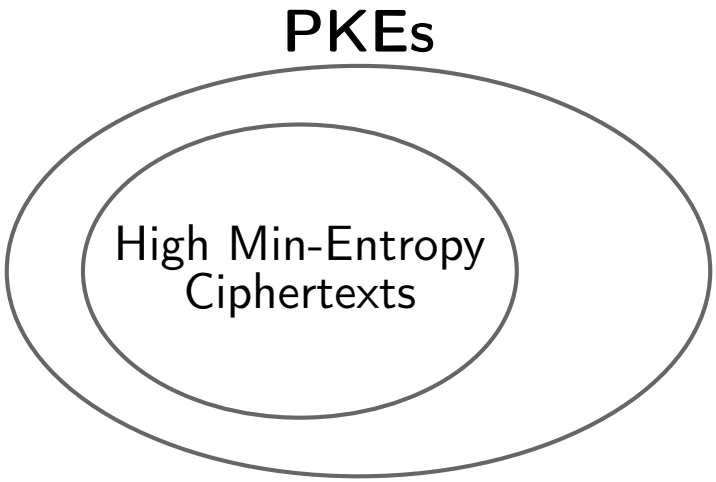
1. $c \leftarrow \mathsf{E.Enc}(\mathsf{pk}, m)$
2. **if** $\mathsf{PRF}(\mathsf{dk}, c) \neq \widehat{m}$: **retry**
3. **else**: **return** c

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

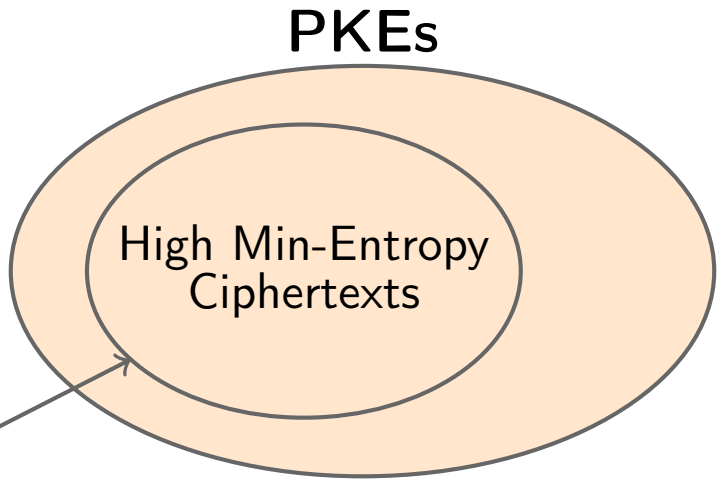
1. $\widehat{m} \leftarrow \mathsf{PRF}(\mathsf{dk}, c)$
2. **return** $\widehat{m}$

- Works **for almost* any** secure and correct PKE!
- * If for all m, $\mathrm{H}_\infty(\mathsf{E.Enc}(\mathsf{pk}, m)) = \omega(\log \lambda)$
- It is Semi-Adaptive for any secure and correct PKE!
- Supports $O(\log \lambda)$ bits long messages.

Anamorphic Limits overview

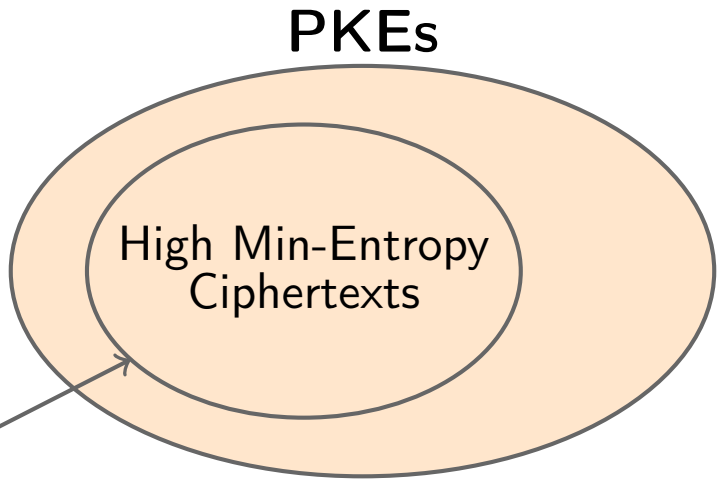


Anamorphic Limits overview



[CGM24b]:
$|\widehat{m}| = O(\log \lambda)$
(black-box)
Tight result

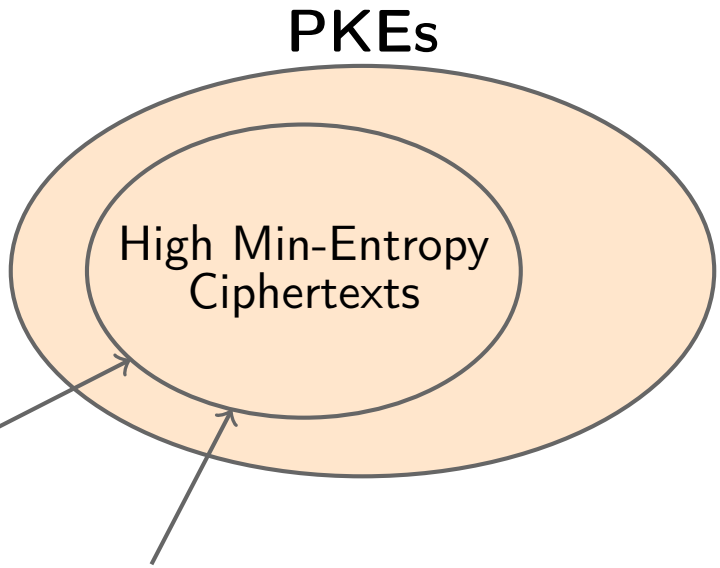
Anamorphic Limits overview



[CGM24b]:
$|\widehat{m}| = O(\log \lambda)$
(black-box)
Tight result

[This work]:
Extends to SA-AE
Verifiable VBB
Obfuscation does not help

Anamorphic Limits overview

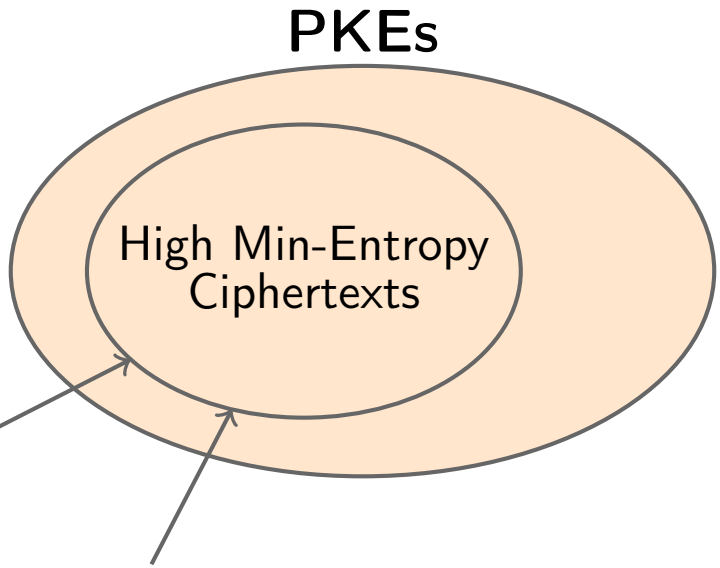


[CGM24b]:
$|\widehat{m}| = O(\log \lambda)$
(black-box)
Tight result

[CGM24b]:
Asymmetric AE
is impossible
(black-box)

[This work]:
Extends to SA-AE
Verifiable VBB
Obfuscation does not help

Anamorphic Limits overview



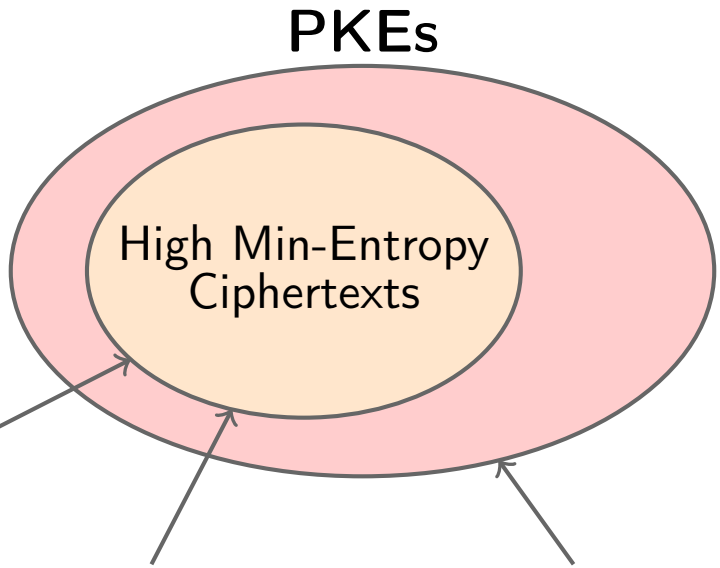
[CGM24b]:
$|\widehat{m}| = O(\log \lambda)$
(black-box)
Tight result

[CGM24b]:
Asymmetric AE
is impossible
(black-box)

[This work]:
Extends to SA-AE
Verifiable VBB
Obfuscation does not help

[This work]:
Extends to
SA-AE

Anamorphic Limits overview



[CGM24b]:
$|\widehat{m}| = O(\log \lambda)$
(black-box)
Tight result

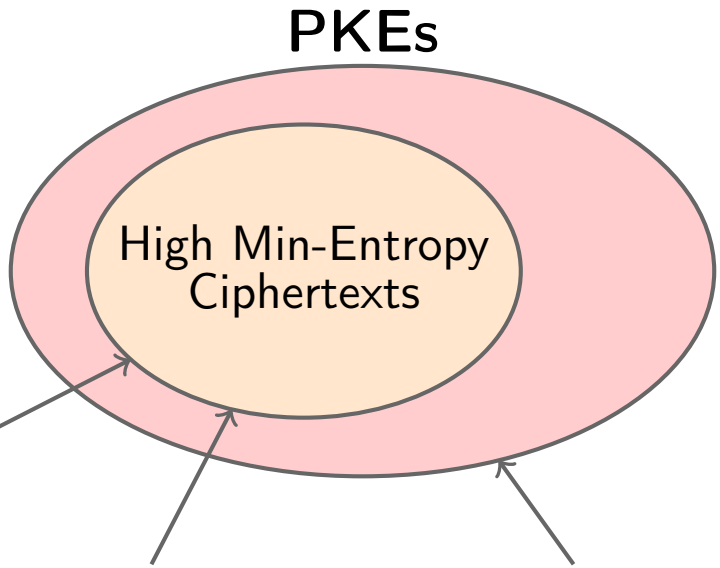
[CGM24b]:
Asymmetric AE
is impossible
(black-box)

[This work]:
Stateless AE
is impossible
(black-box and
bb + VVBB)

[This work]:
Extends to SA-AE
Verifiable VBB
Obfuscation does not help

[This work]:
Extends to
SA-AE

Anamorphic Limits overview



[CGM24b]:
$|\widehat{m}| = O(\log \lambda)$
(black-box)
Tight result

[CGM24b]:
Asymmetric AE
is impossible
(black-box)

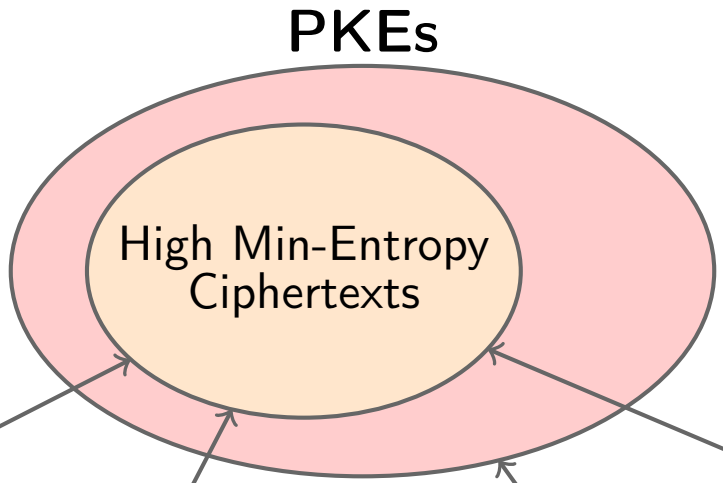
[This work]:
Stateless AE
is impossible
(black-box and
bb + VVBB)

[This work]:
Extends to SA-AE
Verifiable VBB
Obfuscation does not help

[This work]:
Extends to
SA-AE

[This work]:
Asymmetric SA-AE
$|\widehat{m}| = \Theta(\log \lambda)$
(from iO)

Anamorphic Limits overview



[CGM24b]:
$|\widehat{m}| = O(\log \lambda)$
(black-box)
Tight result

[CGM24b]:
Asymmetric AE
is impossible
(black-box)

[This work]:
Stateless AE
is impossible
(black-box and
bb + VVBB)

[This work]:
Asymmetric AE
$|\widehat{m}| = \Theta(\log \lambda)$
(from iO)

[This work]:
Extends to SA-AE
Verifiable VBB
Obfuscation does not help

[This work]:
Extends to
SA-AE

[This work]:
Asymmetric SA-AE
$|\widehat{m}| = \Theta(\log \lambda)$
(from iO)

Q & A

Thanks for your attention

Any questions?

ia.cr/2024/1119