Anamorphic Resistant Encryption: the Good, the Bad and the Ugly

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

[1]University of Catania, Italy.

[2]IMDEA Software Institute, Madrid, Spain.

[3]Universidad Politecnica de Madrid, Madrid, Spain.

CRYPTO 2025

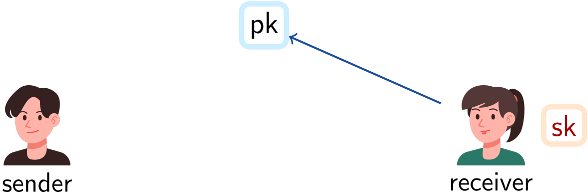
Introduction

Introduction

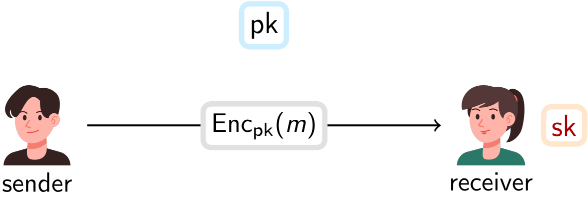

sender


receiver

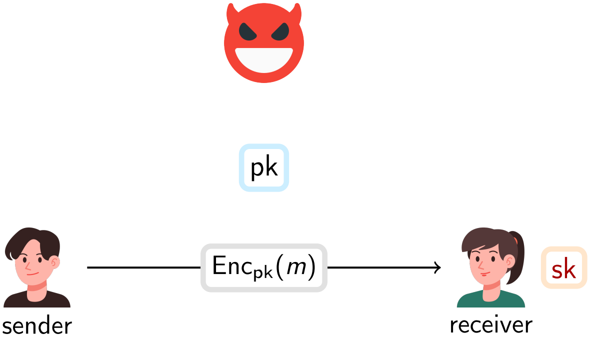
Introduction



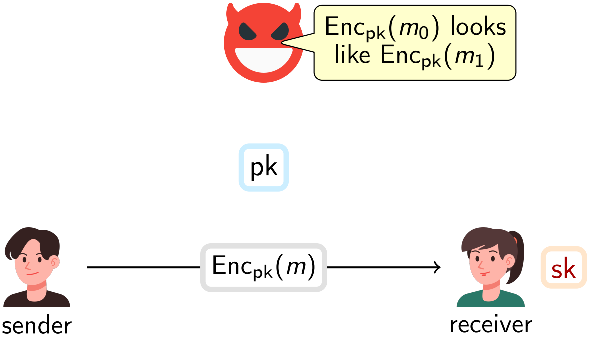
Introduction



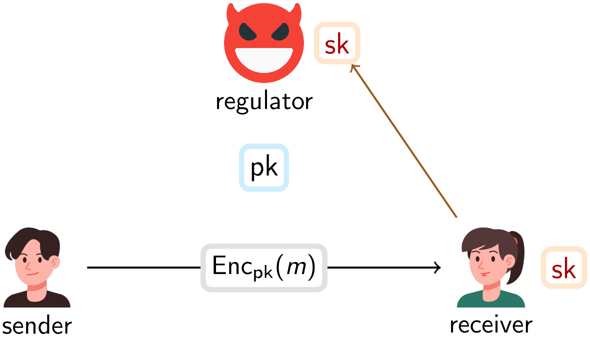
Introduction



Introduction

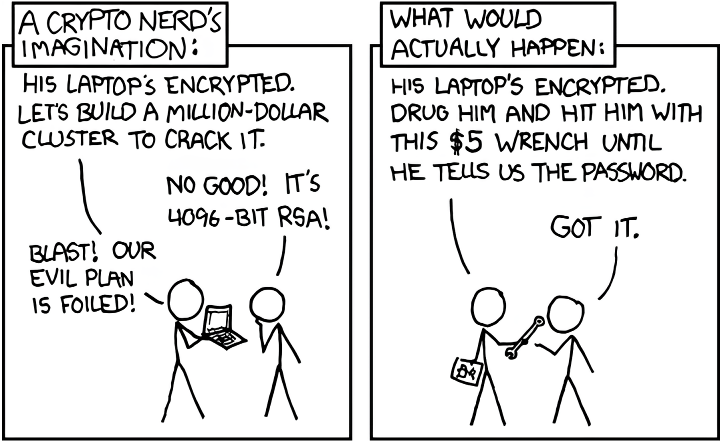


Introduction



Implicit assumption

Receiver privacy assumption



Anamorphic Encryption

Anamorphic Encryption Definition [PPY22]

AT.Gen AT.Enc AT.Dec

Anamorphic Encryption Definition [PPY22]

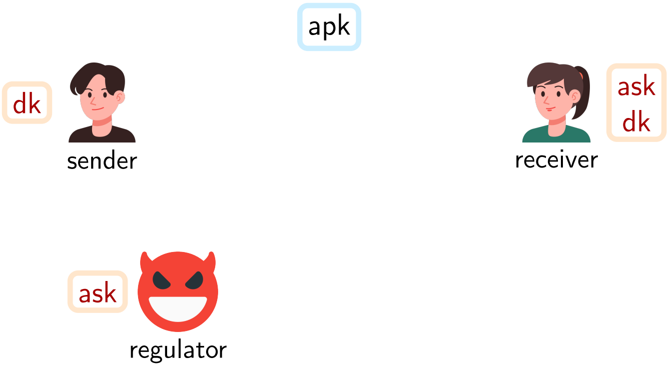
AT.Gen AT.Enc AT.Dec

sender

receiver

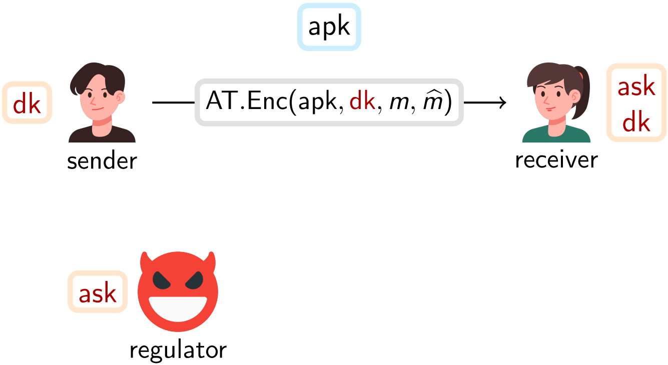
regulator

AT.Gen AT.Enc AT.Dec



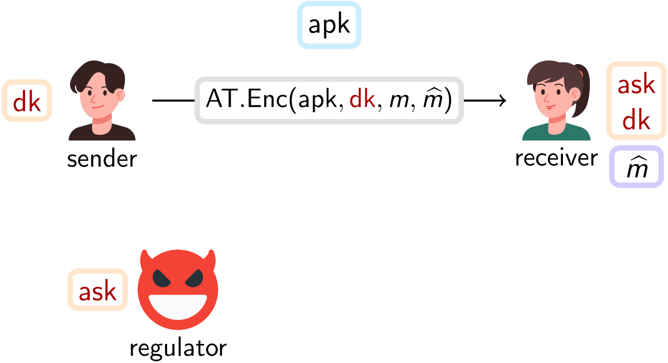
Anamorphic Encryption Definition [PPY22]

AT.Gen AT.Enc AT.Dec



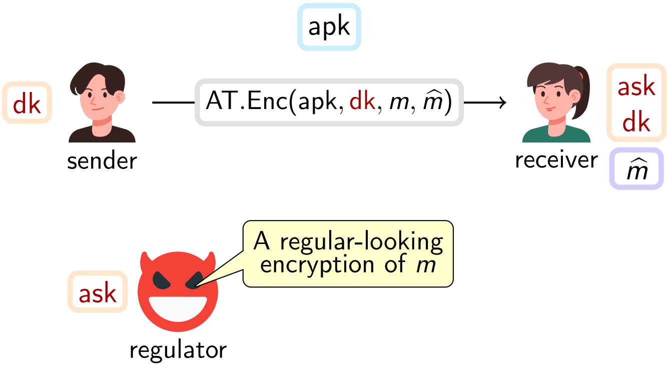
Anamorphic Encryption Definition [PPY22]

AT.Gen AT.Enc AT.Dec



Anamorphic Encryption Definition [PPY22]

AT.Gen AT.Enc AT.Dec



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

$\mathsf{pk}, \mathsf{sk} \leftarrow \mathsf{E.Gen}(\lambda)$

pk, sk

$(m, \widehat{m})$

$c \leftarrow \mathsf{E.Enc}(\mathsf{pk}, m)$

c

Anamorphic Game

$\mathsf{apk}, \mathsf{ask}, \mathsf{dk} \leftarrow \mathsf{AT.Gen}(\lambda)$

$\mathsf{apk}, \mathsf{ask}$

$(m, \widehat{m})$

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

c

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

Constructions

Specific:

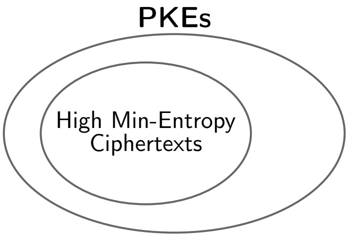
- Naor-Yung transform [PPY22]
- Selective Randomness Recoverability [BGHM24, KPPY23]
- Hybrid Encryption [CGM24a]
- Specific schemes (e.g., ElGamal, Cramer-Shoup, GSW)
- Reduction properties [PPY24]

Generic:

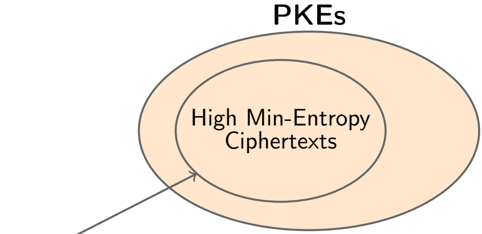
- Rejection Sampling (RS) [PPY22]

Limits of Anamorphic Encryption

Limits of Anamorphic Encyrption overview

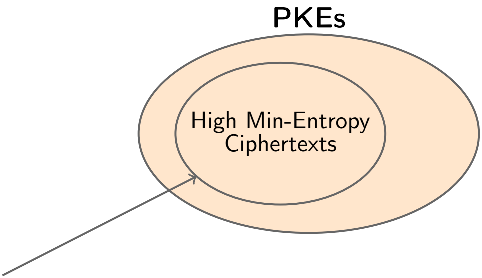


Limits of Anamorphic Encryption overview



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

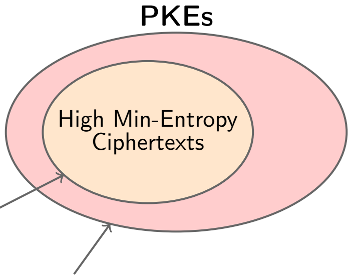
Limits of Anamorphic Encyrption overview



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

[CGM25]:
Verifiable VBB
does not help

Limits of Anamorphic Encyrption overview

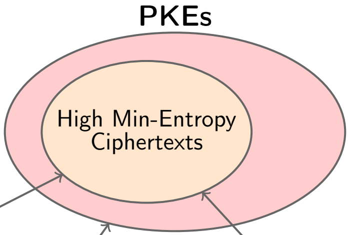


[CGM24b]:
$|\widehat{m}| = O(\log \lambda)$
(black-box)
Tight result

[CGM25]:
Stateless AE
is impossible
(black-box and
VVBB does not help)

[CGM25]:
Verifiable VBB
does not help

Limits of Anamorphic Encyrption overview



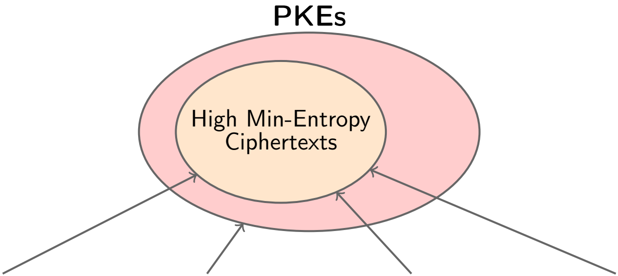
[CGM24b]:
$|\widehat{m}| = O(\log \lambda)$
(black-box)
Tight result

[CGM25]:
Verifiable VBB
does not help

[CGM25]:
Stateless AE
is impossible
(black-box and
VVBB does not help)

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

Limits of Anamorphic Encyrption overview



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

[CGM25]:
Verifiable VBB
does not help

[CGM25]:
Stateless AE
is impossible
(black-box and
VVBB does not help)

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

[CGM25]:
Asymmetric AE
$|\widehat{m}| = \Theta(\log \lambda)$
(from iO)

Question

The above results apply *only* to black-box constructions. The following two statements do not directly contradict state of the art results:

- *Every* semantically secure PKE can support a stateless secure AE scheme.
- There exists a concrete PKE such that no stateless anamorphic triplet is secure with respect to it.

A natural question is, therefore, to settle this state of things in one direction or the other.

Anamorphic Resistant Encryption

- In [DG25] an ARE is a secure PKE for which it holds that for any AE then $|\widehat{m}| = O(\log \lambda)$.
  - ARE notion introduced.
  - Shows a concrete PKE for which results from [CGM24b] hold.
  - Actually an independent work from [CGM24b].

Anamorphic Resistant Encryption

- In [DG25] an ARE is a secure PKE for which it holds that for any AE then $|\widehat{m}| = O(\log \lambda)$.
  - ARE notion introduced.
  - Shows a concrete PKE for which results from [CGM24b] hold.
  - Actually an independent work from [CGM24b].
- In [This work] an ARE is a secure PKE for which it holds that for any AE then $|\widehat{m}| = 0$.
  - Shows a concrete PKE for which results from [CGM25] hold.
  - Actually an independent work from [DG25], but name taken from there.

The Bad and the Ugly

Our main contribution

We give two concrete compilers transforming essentially any PKE with large message space into an ARE

- Our first construction
  - is in the public parameters model;
  - makes use of injective OWF, iO and Extremely Lossy Function (ELF).

Our main contribution

We give two concrete compilers transforming essentially any PKE with large message space into an ARE

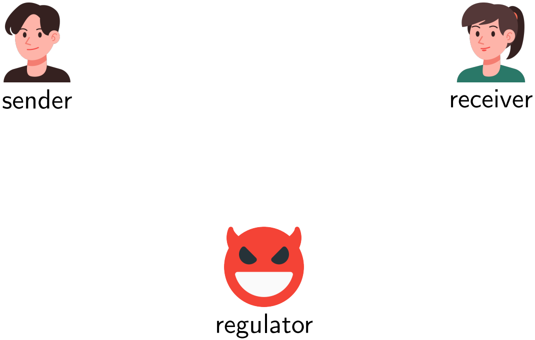
- Our first construction
  - is in the public parameters model;
  - makes use of injective OWF, iO and Extremely Lossy Function (ELF).
- Our second construction
  - does not need public parameters;
  - does not need iO;
  - ...but it is in the random oracle model.

Public Parameters Model

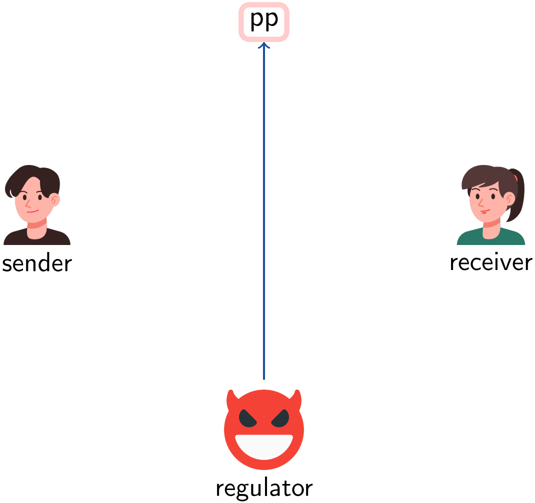
sender

receiver

Public Parameters Model



Public Parameters Model



Public Parameters Model

pp

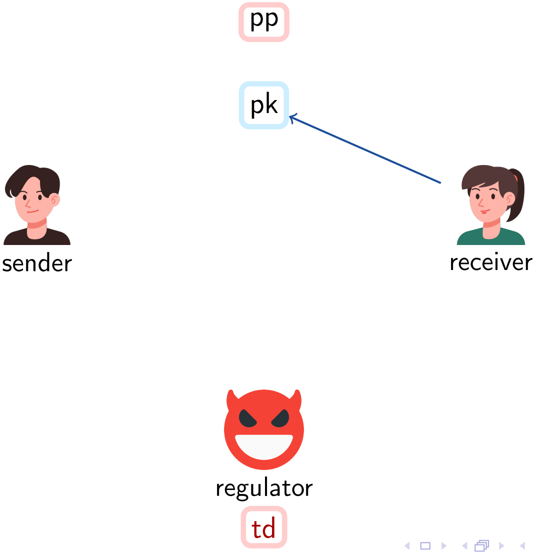
sender

receiver

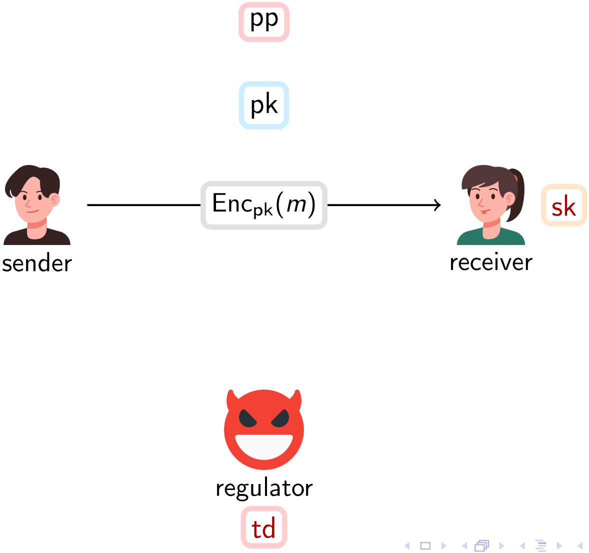
regulator

td

Public Parameters Model



Public Parameters Model



Our starting point: Weak Messages [CGM25]

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

Construction in Public Parameters Model - Sketch

Construction in Public Parameters Model - Sketch

E.Init(λ) :

1. Sample $m_1^*, \ldots, m_\lambda^* \xleftarrow{\$} M$ distinct
2. Compute $z_i \leftarrow F(m_i^*)$
3. Generate $f_i \xleftarrow{\$}$ ELF.Gen$(2^\mu, 2^i)$
4. $\widetilde{C} \leftarrow \mathsf{iO}(C_{\mathsf{z},\mathsf{f}})$
5. **return** $(\mathsf{pp}, \mathsf{td}) \leftarrow (\widetilde{C}, (m_i^*)_{i=1}^{\lambda})$

$C_{\mathsf{z},\mathsf{f}}(m)$:

1. **if** $F(m) = z_i$: $f \leftarrow f_i$
2. **else**: $f \leftarrow$ ELF.Gen$(2^\mu, 2^\mu)$
3. **return** f

Construction in Public Parameters Model - Sketch

$\mathsf{E.Init}(\lambda)$:
1. Sample $m_1^*, \ldots, m_\lambda^* \xleftarrow{\$} M$ distinct
2. Compute $z_i \leftarrow F(m_i^*)$
3. Generate $f_i \xleftarrow{\$} \mathsf{ELF.Gen}(2^\mu, 2^i)$
4. $\widetilde{C} \leftarrow \mathsf{iO}(C_{\mathsf{z},\mathsf{f}})$
5. **return** $(\mathsf{pp}, \mathsf{td}) \leftarrow (\widetilde{C}, (m_i^*)_{i=1}^{\lambda})$

$C_{\mathsf{z},\mathsf{f}}(m)$:
1. **if** $F(m) = z_i$: $f \leftarrow f_i$
2. **else**: $f \leftarrow \mathsf{ELF.Gen}(2^\mu, 2^\mu)$
3. **return** f

$\mathsf{E.Enc}(\mathsf{pp}, \mathsf{pk}, m; r)$:
1. $f \leftarrow \widetilde{C}(m)$
2. $c \leftarrow \mathsf{E.Enc}^*(\mathsf{pk}, m; f(r))$
3. **return** c

IND-CPA proof idea

- OWF protects weak messages
- iO + ELF masks different behavior
- IND-CPA of the underlying PKE

IND-CCA is achieved in the same way since sk is available in the reductions between hybrids.

ARE - adversary

regulator

challenger

ARE - adversary

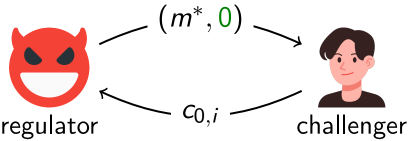
$$m_j^* \leftarrow \mathsf{td}$$
$$f_j \leftarrow \widehat{C}(m_j^*)$$
$$R = |\{Im\ f_j\}|$$

regulator

challenger

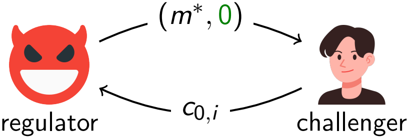
ARE - adversary

$$m_j^* \leftarrow \mathrm{td}$$
$$f_j \leftarrow \widehat{C}(m_j^*)$$
$$R = |\{Im\ f_j\}|$$



ARE - adversary

$$m_j^* \leftarrow \mathrm{td}$$
$$f_j \leftarrow \widehat{C}(m_j^*)$$
$$R = |\{Im\ f_j\}|$$



Store $c_{0,i}$ in S_0

ARE - adversary

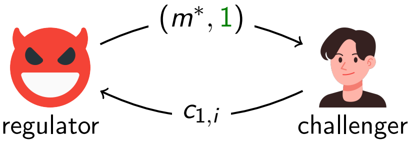
$$m_j^* \leftarrow \mathsf{td}$$
$$f_j \leftarrow \widehat{C}(m_j^*)$$
$$R = |\{Im\ f_j\}|$$

regulator

challenger

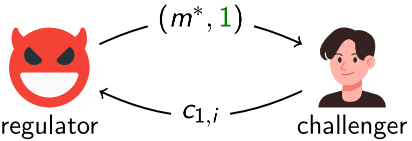
ARE - adversary

$$m_j^* \leftarrow \mathrm{td}$$
$$f_j \leftarrow \widehat{C}(m_j^*)$$
$$R = |\{Im\ f_j\}|$$



ARE - adversary

$$m_j^* \leftarrow \mathrm{td}$$
$$f_j \leftarrow \widehat{C}(m_j^*)$$
$$R = |\{Im\ f_j\}|$$



Store $c_{1,i}$ in S_1

ARE - adversary

$$m_j^* \leftarrow \mathrm{td}$$
$$f_j \leftarrow \widehat{C}(m_j^*)$$
$$R = |\{Im\ f_j\}|$$

regulator

challenger

return $(|S_0| == R) \wedge (|S_1| == R)$

The Good

ASA Definition [BPR14, WHCY23]

sender

receiver

ASA Definition [BPR14, WHCY23]

ASA Definition [BPR14, WHCY23]

ASA.Gen ASA.Enc ASA.Ext

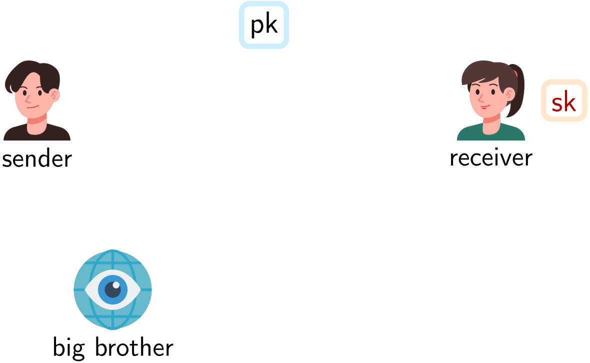
sender

receiver

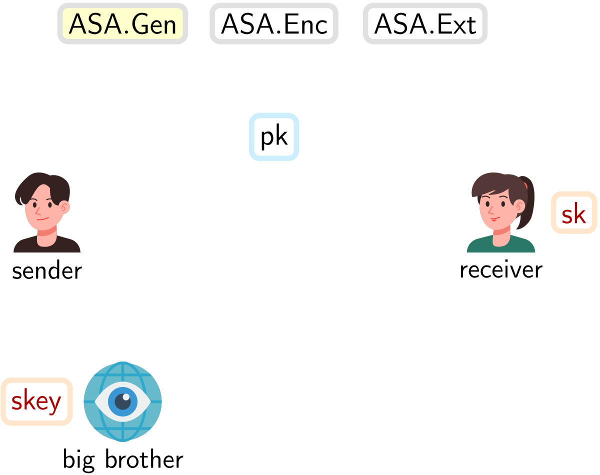
big brother

ASA Definition [BPR14, WHCY23]

ASA.Gen ASA.Enc ASA.Ext



ASA Definition [BPR14, WHCY23]



ASA Definition [BPR14, WHCY23]

ASA.Gen ASA.Enc ASA.Ext

pk


sender

— ASA.Enc(pk, skey, m, $\widehat{m}$) ⟶


receiver

sk

skey


big brother

ASA Definition [BPR14, WHCY23]

ASA.Gen ASA.Enc ASA.Ext

pk

sender

$\longrightarrow$ ASA.Enc(pk, skey, m, $\widehat{m}$) $\longrightarrow$

receiver

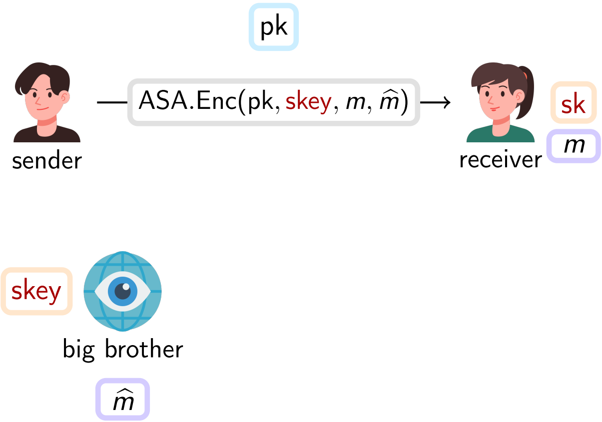
sk

m

skey

big brother

ASA.Gen ASA.Enc ASA.Ext



ASA Definition [BPR14, WHCY23]

ASA.Gen ASA.Enc ASA.Ext

pk

A regular-looking encryption of m

sender

$\longrightarrow$ $\mathsf{ASA.Enc}(\mathsf{pk}, \mathsf{skey}, m, \widehat{m})$ $\longrightarrow$

receiver

sk

m

skey

big brother

$\widehat{m}$

Connection with ASA

We establish a strong connection between ASA on PKE and Anamorphic Encryption

- Algorithm Substitution Attack $\implies$ Anamorphic Encryption
- Anamorphic Encryption $\implies$ Algorithm Substitution Attack

ASA resistant encryption until now:

- Deterministic schemes
- IND-CPA:
  - Non-black-box techniques
  - Trust assumptions

Reinterpretation of ARE

ASA resistant encryption until now:

- Deterministic schemes
- IND-CPA:
  - Non-black-box techniques
  - Trust assumptions

Our AREs properties:

- IND-CCA
- Homomorphic
- Black-box

Thanks for your attention!

ia.cr/2025/233