Anamorphic Encryption: New Constructions and Homomorphic Realizations

Dario Catalano[1] Emanuele Giunta[2, 3, 4] Francesco Migliaro[1]

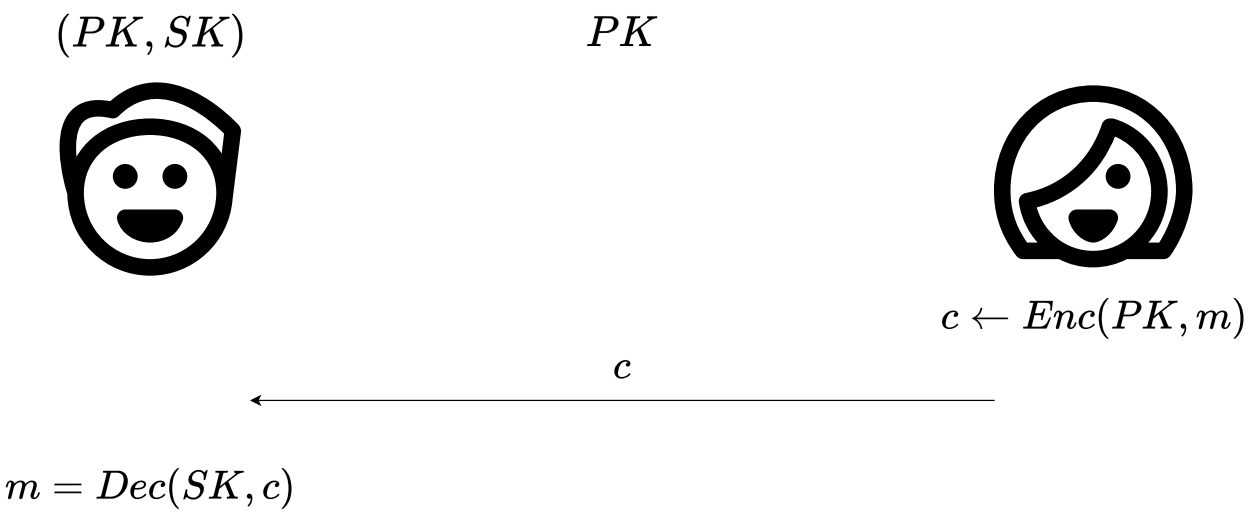
[1]Università di Catania, Italy.

[2]IMDEA Software Institute, Madrid, Spain.

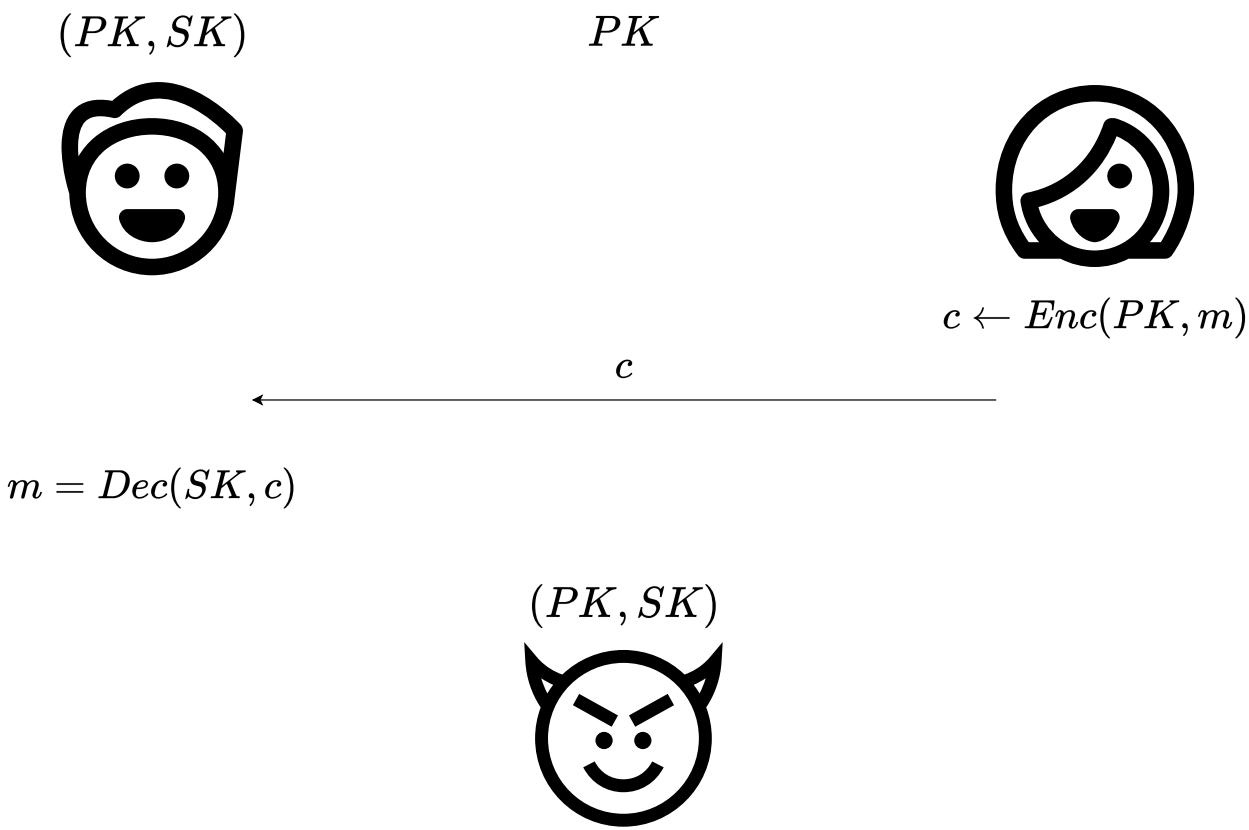
[3]Universidad Politecnica de Madrid, Spain.

[4]Web 3.0 Foundation, Zug, Switzerland.

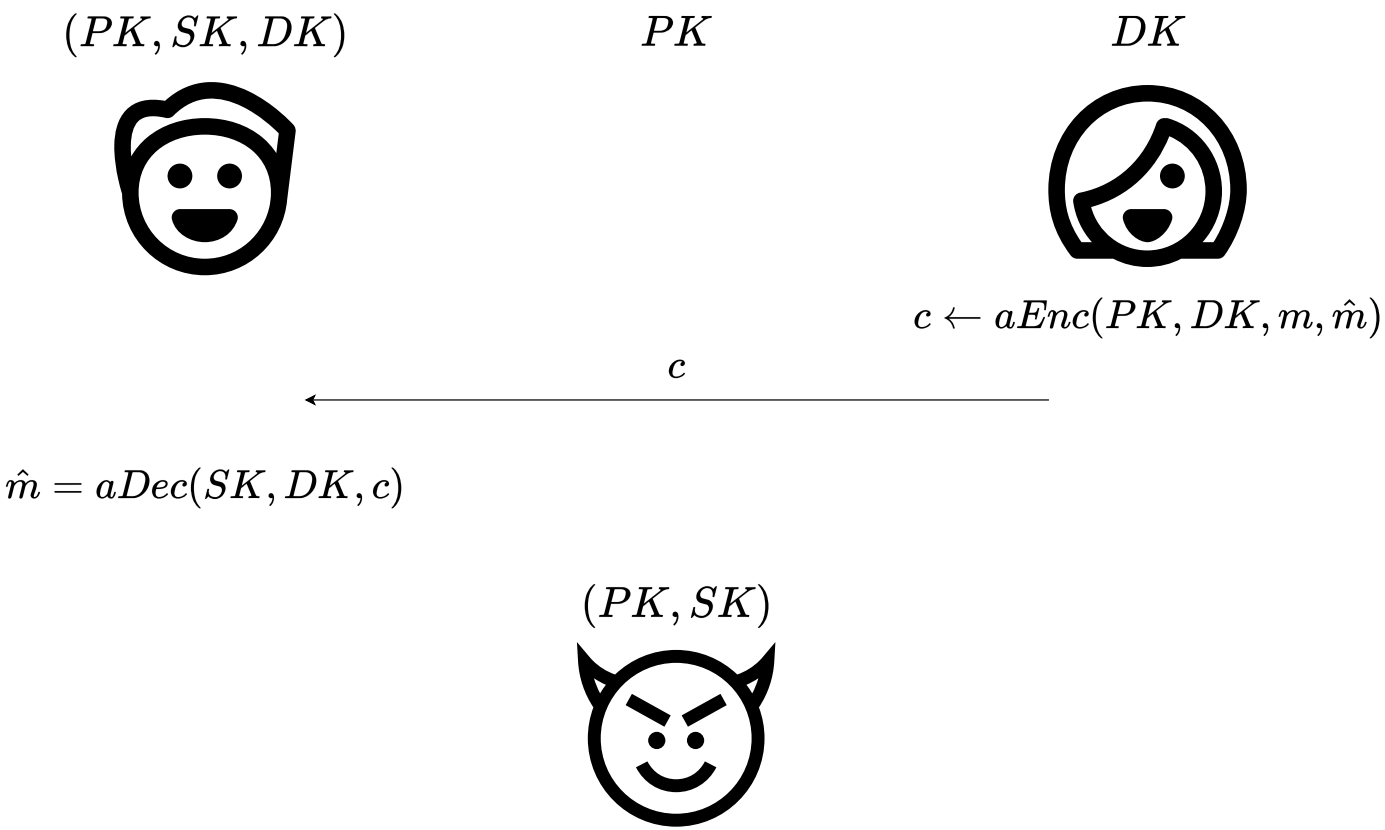
PKE



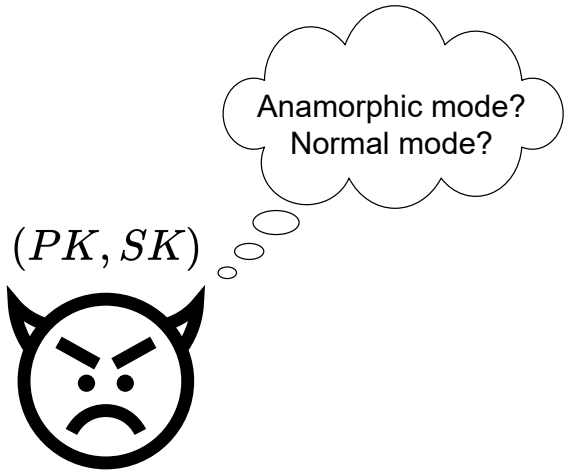
Anamorphic Encryption [PPY22]



Anamorphic Encryption [PPY22]



Anamorphic Encryption [PPY22]



Normal$(\lambda, \mathcal{A})$

1 : $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KGen}(\lambda)$
2 : When $(m, \widehat{m}) \leftarrow \mathcal{A}(\mathsf{pk}, \mathsf{sk})$
3 : Sample a random r
4 : Give $\mathsf{Enc}(\mathsf{pk}, m; r)$ to $\mathcal{A}$

Anamorphic$(\lambda, \mathcal{A})$

1 : $(\mathsf{pk}, \mathsf{sk}, \mathsf{dk}) \leftarrow \mathsf{aGen}(\lambda)$
2 : When $(m, \widehat{m}) \leftarrow \mathcal{A}(\mathsf{pk}, \mathsf{sk})$
3 : Sample a random r
4 : Give $\mathsf{aEnc}(\mathsf{pk}, \mathsf{dk}, m, \widehat{m}; r)$ to $\mathcal{A}$

Our Contribution

- Novel generic examples of anamorphism
- Refined notion
- Anamorphic Encryption with Homomorphic properties

This talk

- Hybrid Encryption is Anamorphic
- Fully Asymmetric anamorphism
- Anamorphic GSW with homomorphic properties

Hybrid Encryption

Ingredients:

- A Public Key Encryption (PKE)
- A Secret Key Encryption (SKE)

$\mathsf{Enc}(\mathsf{pk}, m)$

1 : $k \leftarrow \mathsf{SKE.KGen}(\lambda)$
2 : $\mathsf{ct}_m \leftarrow \mathsf{SKE.Enc}(k, m)$
3 : $\mathsf{ct}_k \leftarrow \mathsf{PKE.Enc}(\mathsf{pk}, k)$
4 : return $\mathsf{ct} = (\mathsf{ct}_m, \mathsf{ct}_k)$

$\mathsf{Dec}(\mathsf{sk}, \mathsf{ct})$

1 : $k = \mathsf{PKE.Dec}(\mathsf{sk}, \mathsf{ct}_k)$
2 : $m = \mathsf{SKE.Dec}(k, \mathsf{ct}_m)$
3 : return m

Anamorphic Hybrid Encryption

Ingredients:

- A Secret Key Encryption with pseudorandom ciphertexts (prE)

$\mathsf{aEnc}(\mathsf{pk}, \mathsf{dk}, m, \widehat{m})$

1 : $k \leftarrow \mathsf{prE.Enc}(\widehat{k}, \widehat{m})$

2 : $\mathsf{ct}_m \leftarrow \mathsf{SKE.Enc}(k, m)$

3 : $\mathsf{ct}_k \leftarrow \mathsf{PKE.Enc}(\mathsf{pk}, k)$

4 : return $c = (\mathsf{ct}_m, \mathsf{ct}_k)$

$\mathsf{aDec}(\mathsf{sk}, \mathsf{dk}, c)$

1 : $k = \mathsf{PKE.Dec}(\mathsf{sk}, \mathsf{ct}_k)$

2 : $\widehat{m} = \mathsf{prE.Dec}(\widehat{k}, k)$

3 : return $\widehat{m}$

Why does this work?

Break anamorphism $\Longrightarrow$ break pseudorandomness of ciphertexts

Previous works limitations

- dk acts as symmetric key $\Longrightarrow$ $\widehat{m}$ can be retrieved by any dk holder
- Multiple covert channels $\Longrightarrow$ different dk for each channel

Refined Anamorphic Encryption

(PK, SK, DK, TK) PK DK

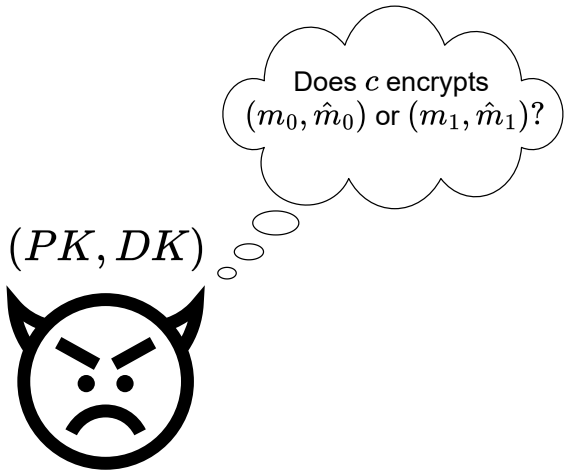
$c \leftarrow aEnc(PK, DK, m, \hat{m})$

c

$\hat{m} = aDec(SK, TK, c)$

(PK, SK)

Fully Asymmetric AE



FAsyAnam-IND-CPA$^b(\mathcal{A})$

1 : $(\mathsf{apk}, \mathsf{ask}, \mathsf{dk}, \mathsf{tk}) \leftarrow \mathsf{aGen}(\lambda)$

2 : $(m_0, m_1, \widehat{m}_0, \widehat{m}_1) \leftarrow \mathcal{A}(\mathsf{apk}, \mathsf{dk})$

3 : $c \leftarrow \mathsf{aEnc}(\mathsf{apk}, \mathsf{dk}, m_b, \widehat{m}_b)$

Homomorphic Encryption

- KGen
- Enc
- Dec
- Eval

$$\mathsf{Eval}(f, \mathsf{Enc}(m_1), \mathsf{Enc}(m_2)) \rightarrow \mathsf{Enc}(f(m_1, m_2))$$

Homomorphic Anamorphic Encryption

- KGen - aGen
- Enc - aEnc
- Dec - aDec
- Eval

$$\mathsf{Eval}(f, \mathsf{aEnc}(m_1, \widehat{m}_1), \mathsf{aEnc}(m_2, \widehat{m}_2)) \rightarrow \mathsf{aEnc}(f(m_1, m_2), f(\widehat{m}_1, \widehat{m}_2))$$

GSW

KGen(λ)

1 : pk is an LWE sample (b, B)

2 : sk is a vector $(1, -t)$

Enc(pk, m)

1 : R is a random binary matrix

2 : $C = m \cdot I_N + RA$

3 : return C

Dec(sk, C)

1 : Let $\mathsf{v} = \mathsf{sk}$

2 : if $C\mathsf{v} = m\mathsf{v} + \mathsf{e}'$ with suitably short e':

3 : Extract and return m

Anamorphic GSW

aGen(λ)

1 : B is a LWE sample $(b_2, \widetilde{B})$
2 : pk $= (b_1, B)$
3 : sk is a vector $(1, -t_1)$
4 : dk $= (P_1, P_2, (0, 1, -t_2))$

aEnc(pk, dk, m, $\widehat{m}$)

1 : Let $A =$ pk
2 : R is a random binary matrix
3 : $C = mP_1 + \widehat{m}P_2 + RA$
4 : return C

aDec(sk, dk, C)

1 : Let $\mathsf{v}_2 = (0, 1, -t_2)$
2 : if $C\mathsf{v}_2 = \widehat{m}\mathsf{v}_2 + \mathsf{e}'$ with suitably short e':
3 : Extract and return $\widehat{m}$

Anamorphic GSW

$$P_i \mathsf{v}_j = \begin{cases} \mathsf{v}_i \text{ if } i = j \\ 0 \text{ else} \end{cases}$$

By construction $\mathsf{v}_1 = (1, \widetilde{\mathsf{v}}_1)$ and $\mathsf{v}_2 = (0, \widetilde{\mathsf{v}}_2)$:

$$P_1 = (\mathsf{v}_1, \Omega_{N,N-1}) \quad \Longrightarrow \quad \begin{cases} P_1 \mathsf{v}_1 = 1 \cdot \mathsf{v}_1 + \Omega_{N,N-1} \widetilde{\mathsf{v}}_1 = \mathsf{v}_1 \\ P_1 \mathsf{v}_2 = 0 \cdot \mathsf{v}_1 + \Omega_{N,N-1} \widetilde{\mathsf{v}}_2 = 0. \end{cases}$$

$$P_2 = I_N - P_1.$$

Why does this work?

Anamorphism (informal):

- Distinguish regular keys from anamorphic keys $\implies$ break LWE
- Real ciphertext is statistically close to anamorphic ciphertext

Homomorpshim (informal):

- If $C_1 \mathsf{v}_2 = \widehat{m}_1 \mathsf{v}_2 + e_1$ and $C_2 \mathsf{v}_2 = \widehat{m}_2 \mathsf{v}_2 + e_2$ $\implies$ same argument of GSW.

Conclusions and Open Questions

- Anamorphic Encryption exists in a large class of encryption schemes
- Stronger privacy notions can be achieved
- Homomorphism properties can be preserved in AE

Open questions

- Can we make GSW Fully Asymmetric?
- Can we obtain others HAE?

Q & A

Thanks for your attention

Any questions?

ia.cr/2024/486