Searching for ELFs in the Cryptographic Forest

TCC 2023

Marc Fischlin **Felix Rohrbach**

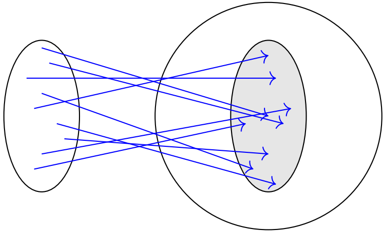
Technische Universität Darmstadt, Germany

Extremely Lossy Functions (ELFs)

Mark Zhandry: The Magic of ELFs, Crypto 2016

Extremely Lossy Functions (ELFs)

Injective Mode

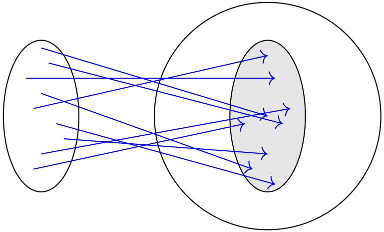


pk_{inj}

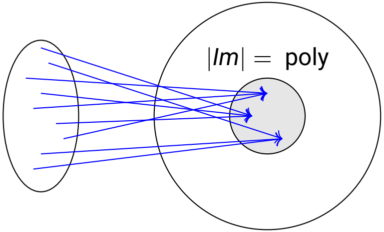
Mark Zhandry: The Magic of ELFs, Crypto 2016

Extremely Lossy Functions (ELFs)

Injective Mode | **(Extremely) Lossy Mode**



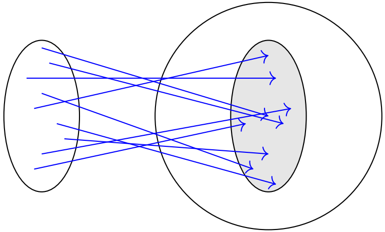
pk_{inj} pk_{loss}



Mark Zhandry: The Magic of ELFs, Crypto 2016

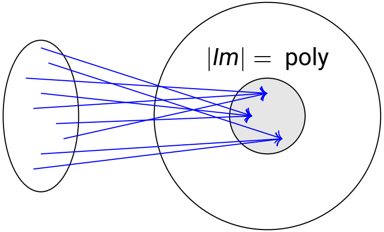
Extremely Lossy Functions (ELFs)

Injective Mode



$$\mathrm{pk}_{\mathrm{inj}} \overset{c}{\approx} \mathrm{pk}_{\mathrm{loss}}$$

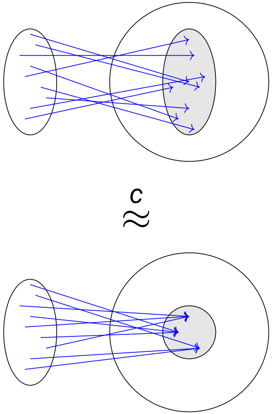
(Extremely) Lossy Mode



Mark Zhandry: The Magic of ELFs, Crypto 2016

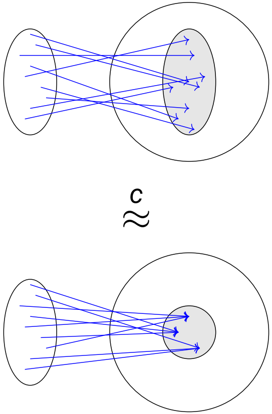
ELFs and the Random-Oracle Model

- ELFs can be used to replace ROM



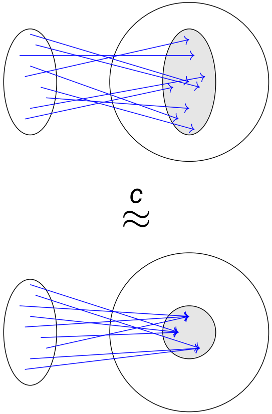
ELFs and the Random-Oracle Model

- ELFs can be used to replace ROM
- Many attempts to replace ROM



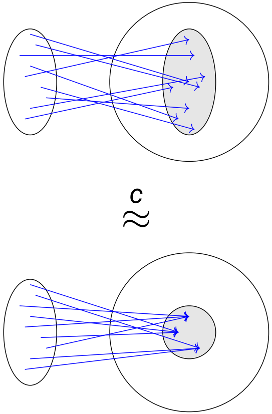
ELFs and the Random-Oracle Model

- ELFs can be used to replace ROM
- Many attempts to replace ROM
  - Correlation Intractability, Universal Computational Extractors



ELFs and the Random-Oracle Model

- ELFs can be used to replace ROM
- Many attempts to replace ROM
  - Correlation Intractability, Universal Computational Extractors
- **Extremely Lossy Functions:**
  - Standard-ish assumptions
  - Useful for many applications



Constructing ELFs

- Exponential decisional *k*-linear assumption:

$$\left(g, g^{a_1}, \ldots, g^{a_k}, g^{\sum_i b_i}, g^{a_1 b_1}, \ldots, g^{a_k b_k}\right) \overset{c_e}{\approx} \left(g, g^{a_1}, \ldots, g^{a_k}, g^{c}, g^{a_1 b_1}, \ldots, g^{a_k b_k}\right)$$

Generalized version of exponential DDH

Mark Zhandry: The Magic of ELFs, Crypto 2016

Constructing ELFs

- Exponential decisional *k*-linear assumption:

$$\left(g, g^{a_1}, \ldots, g^{a_k}, g^{\sum_i b_i}, g^{a_1 b_1}, \ldots, g^{a_k b_k}\right) \stackrel{c_e}{\approx} \left(g, g^{a_1}, \ldots, g^{a_k}, g^{c}, g^{a_1 b_1}, \ldots, g^{a_k b_k}\right)$$

  Generalized version of exponential DDH
- Claim: True for e.g. elliptic curves

Mark Zhandry: The Magic of ELFs, Crypto 2016

Constructing ELFs

- Exponential decisional *k*-linear assumption:

$$\left(g, g^{a_1}, \ldots, g^{a_k}, g^{\sum_i b_i}, g^{a_1 b_1}, \ldots, g^{a_k b_k}\right) \overset{c_e}{\approx} \left(g, g^{a_1}, \ldots, g^{a_k}, g^{c}, g^{a_1 b_1}, \ldots, g^{a_k b_k}\right)$$

  Generalized version of exponential DDH
- Claim: True for e.g. elliptic curves
- Is public-key cryptography necessary?

Mark Zhandry: The Magic of ELFs, Crypto 2016

Constructing ELFs

- Exponential decisional *k*-linear assumption:

$$\left(g, g^{a_1}, \ldots, g^{a_k}, g^{\sum_i b_i}, g^{a_1 b_1}, \ldots, g^{a_k b_k}\right) \overset{c_e}{\approx} \left(g, g^{a_1}, \ldots, g^{a_k}, g^{c}, g^{a_1 b_1}, \ldots, g^{a_k b_k}\right)$$

  Generalized version of exponential DDH
- Claim: True for e.g. elliptic curves
- Is public-key cryptography necessary?
  - Zhandry'16: eOWFs, eCRH might be enough

Mark Zhandry: The Magic of ELFs, Crypto 2016

Constructing ELFs

- Exponential decisional *k*-linear assumption:

$$\left(g, g^{a_1}, \ldots, g^{a_k}, g^{\sum_i b_i}, g^{a_1 b_1}, \ldots, g^{a_k b_k}\right) \overset{c_e}{\approx} \left(g, g^{a_1}, \ldots, g^{a_k}, g^{c}, g^{a_1 b_1}, \ldots, g^{a_k b_k}\right)$$

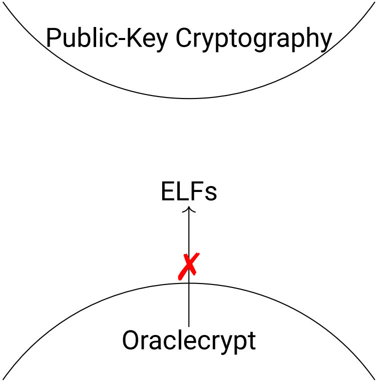
  Generalized version of exponential DDH
- Claim: True for e.g. elliptic curves
- Is public-key cryptography necessary?
  - Zhandry’16: eOWFs, eCRH might be enough
  - Holmgren, Lombardi’18: ELFs from One-Way Product Functions?

Mark Zhandry: The Magic of ELFs, Crypto 2016

What are the minimal assumptions for building ELFs?

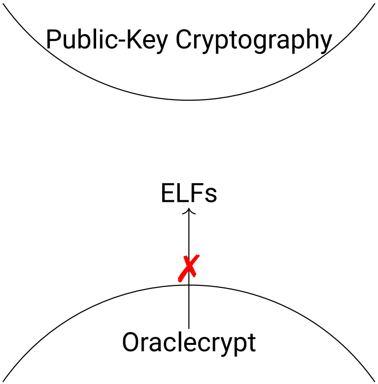
Our Results

- No fully black-box construction of ELFs from eOWFs, eCRHFs, OWPFs, . . .



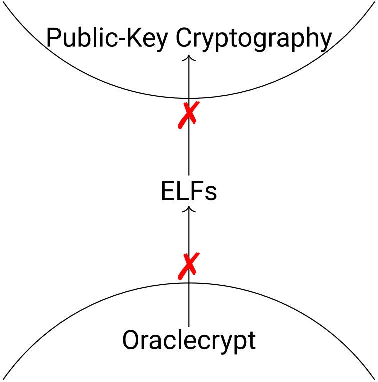
Our Results

- No fully black-box construction of ELFs from eOWFs, eCRHFs, OWPFs, ...
  - Even holds for (moderately) lossy functions!



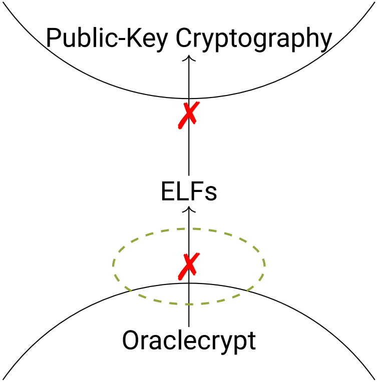
Our Results

- No fully black-box construction of ELFs from eOWFs, eCRHFs, OWPFs, . . .
  - Even holds for (moderately) lossy functions!
- No fully black-box construction of key agreement from ELFs



Our Results

- No fully black-box construction of ELFs from eOWFs, eCRHFs, OWPFs, . . .
  - Even holds for (moderately) lossy functions!
- No fully black-box construction of key agreement from ELFs



Oracle Separation

There exist oracles $\mathcal{O}$, PSPACE^+, such that relative to them:

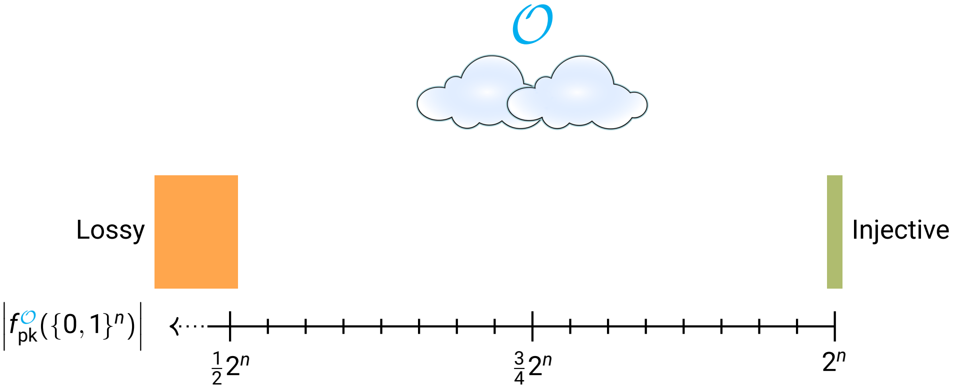
- eOWFs, eCRHFs, OWPFs, $\ldots$ exist,
- but lossy functions and ELFs do not

Oracle Separation

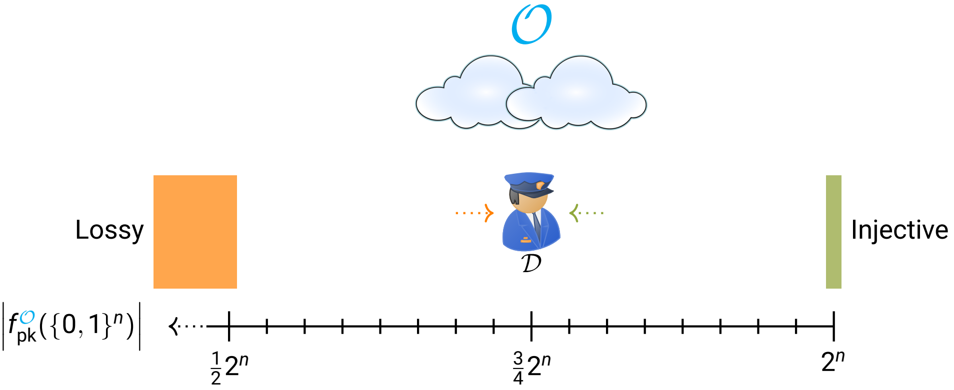
There exist oracles $\mathcal{O}$, PSPACE^+, such that relative to them:

- eOWFs, eCRHFs, OWPFs, $\ldots$ exist,
- but lossy functions and ELFs do not
- Idea similar to *Pietrzak, Rosen, Segev, TCC'12*

Inefficient Distinguisher



Inefficient Distinguisher



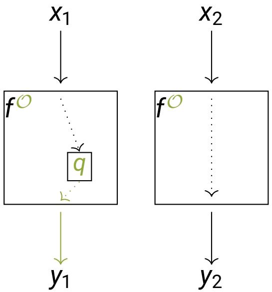
Heavy Queries are Important

- q is *heavy* for f if it appears in $f(x)$ for a poly fraction of all $x \in \{0,1\}^n$

Heavy Queries are Important

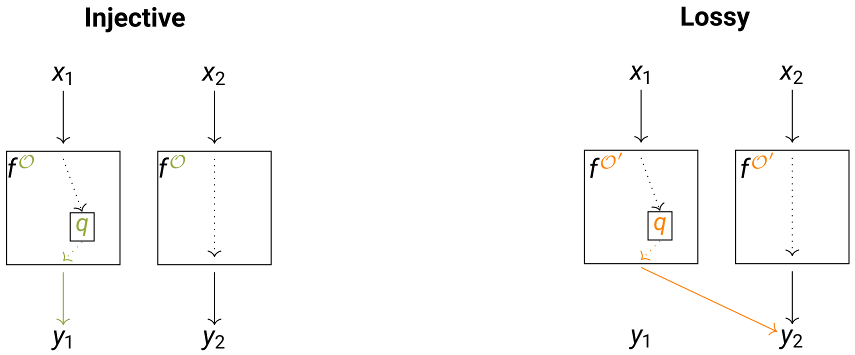
- q is *heavy* for f if it appears in $f(x)$ for a poly fraction of all $x \in \{0,1\}^n$

Injective



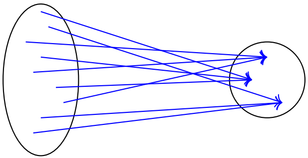
Heavy Queries are Important

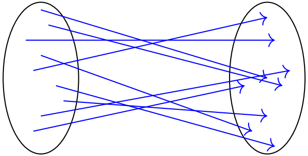
- q is *heavy* for f if it appears in $f(x)$ for a poly fraction of all $x \in \{0,1\}^n$



Observations

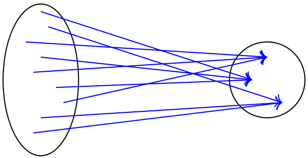
Observation 1: Lossiness is a global property.



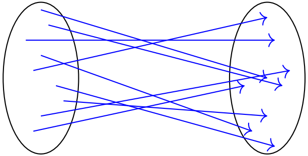


Observations

Observation 1: Lossiness is a global property.

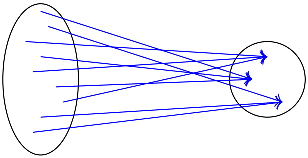


Observation 2: Key generator knows $\mathcal{O}$ at poly many positions



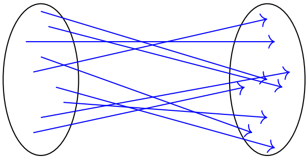
Observations

Observation 1: Lossiness is a global property.



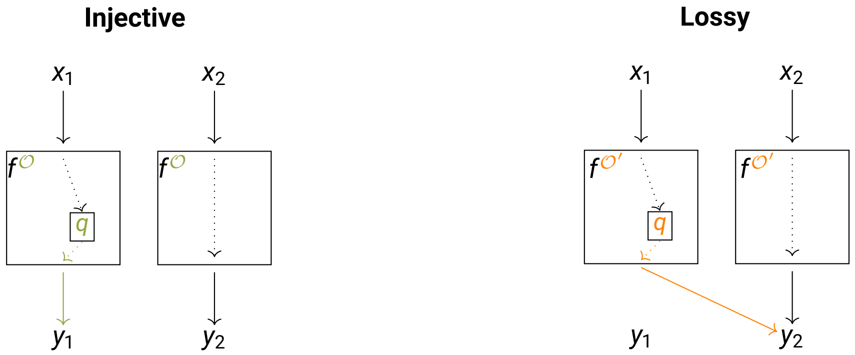
Observation 2: Key generator knows $\mathcal{O}$ at poly many positions

- Other positions cannot influence mode (w.h.p.)

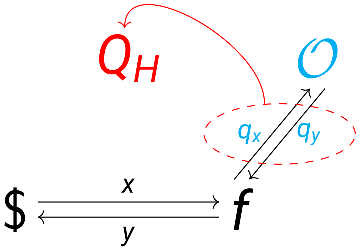


Heavy Queries are Important

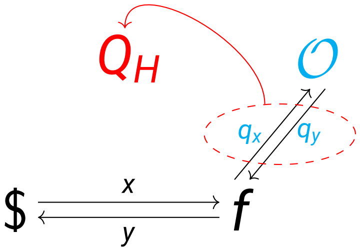
- q is *heavy* for f if it appears in $f(x)$ for a poly fraction of all $x \in \{0,1\}^n$



Heavy Queries are Easy to Find

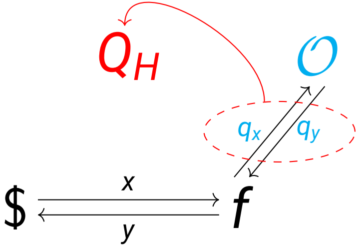


Heavy Queries are Easy to Find



- $|Q_H|$ polynomial

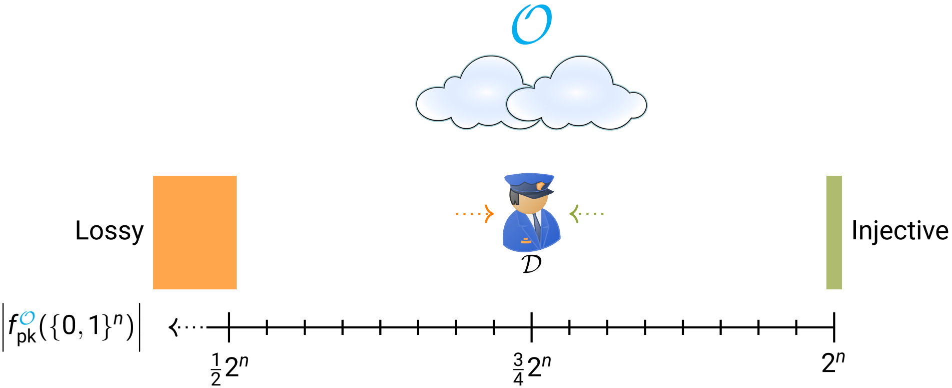
Heavy Queries are Easy to Find



- $|Q_H|$ polynomial
- With overwhelming probability: All heavy queries are in Q_H

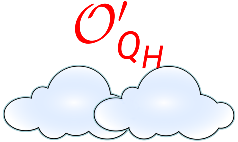
Cryptoplexity
Cryptography & Complexity Theory
Technische Universität Darmstadt
www.cryptoplexity.de

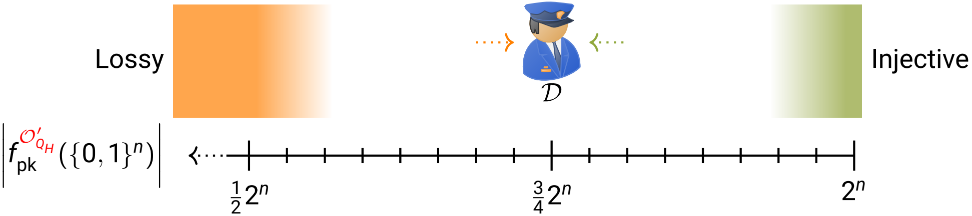
Efficient Distinguisher



Efficient Distinguisher

$$\mathcal{O}'_{Q_H}(x) = \begin{cases} \mathcal{O}(x) & x \in Q_H \\ \mathcal{O}'(x) & x \notin Q_H \end{cases}$$





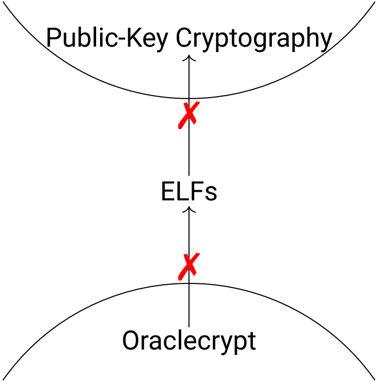
Oracle Separation

There exist oracles $\mathcal{O}$, PSPACE^+, such that relative to them:

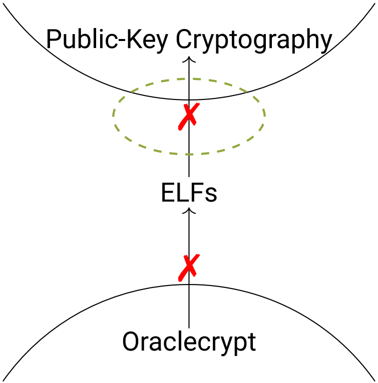
- eOWFs, eCRHFs, OWPFs, . . . exist,
- but lossy functions and ELFs do not

$\Rightarrow$ No fully BB construction of ELFs from anything in Oraclecrypt

Overview



Overview



The Simulation Lemma

- Reuse Impagliazzo–Rudich result (No KA relative to a random permutation)

The Simulation Lemma

- Reuse Impagliazzo–Rudich result (No KA relative to a random permutation)
- Construct (inefficient) ELF oracle $\mathsf{Gen}^{\Pi}, \mathsf{Eval}^{\Pi}$

The Simulation Lemma

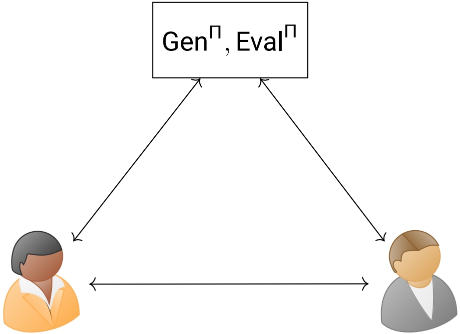
- Reuse Impagliazzo–Rudich result (No KA relative to a random permutation)
- Construct (inefficient) ELF oracle $\mathsf{Gen}^{\Pi}, \mathsf{Eval}^{\Pi}$

Lemma (Simulation Lemma, informal)

There exists an efficient algorithm Wrap^{Π} *such that access to* Wrap^{Π} *or the oracles* $\mathsf{Gen}^{\Pi}, \mathsf{Eval}^{\Pi}$ *is indistinguishable. Further,* Wrap *has no (global) state.*

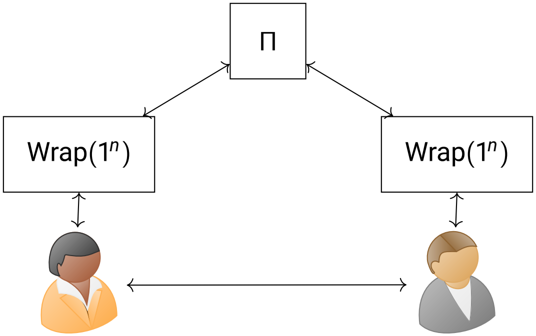
No Key Agreement from ELFs

- Assume KA exists



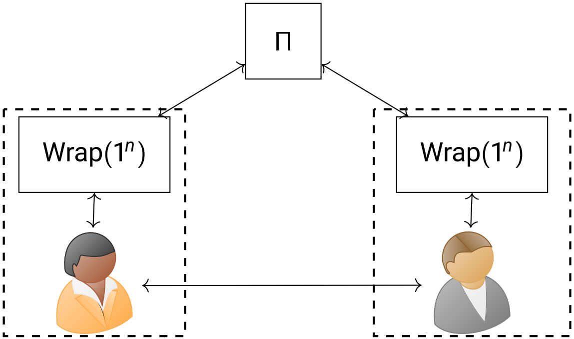
No Key Agreement from ELFs

- Assume KA exists
- Introducing Wrap does not break completeness



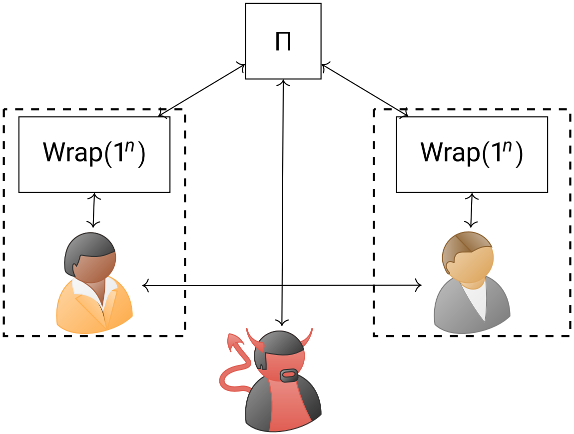
No Key Agreement from ELFs

- Assume KA exists
- Introducing Wrap does not break completeness



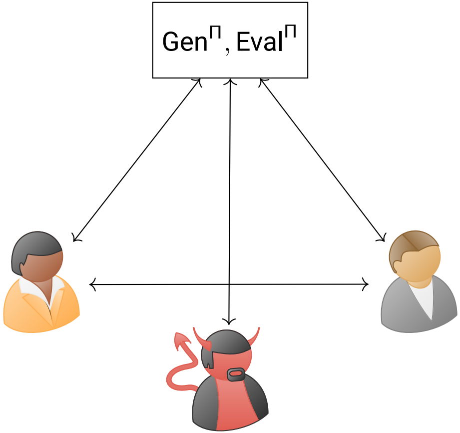
No Key Agreement from ELFs

- Assume KA exists
- Introducing Wrap does not break completeness
- Successful adversary exists (*Impagliazzo, Rudich, STOC'89*)



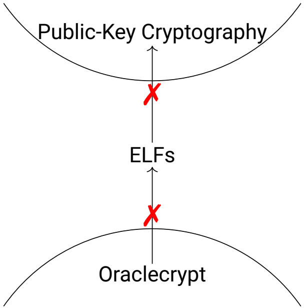
No Key Agreement from ELFs

- Assume KA exists
- Introducing Wrap does not break completeness
- Successful adversary exists (*Impagliazzo, Rudich, STOC'89*)
- Removing Wrap does not break attack ↯



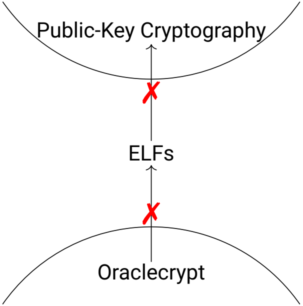
Conclusion

- No fully black-box construction of ELFs from Oraclecrypt primitives
- No fully black-box construction of KA from ELFs



Conclusion

- No fully black-box construction of ELFs from Oraclecrypt primitives
- No fully black-box construction of KA from ELFs



Thank you!

https://ia.cr/2023/1403