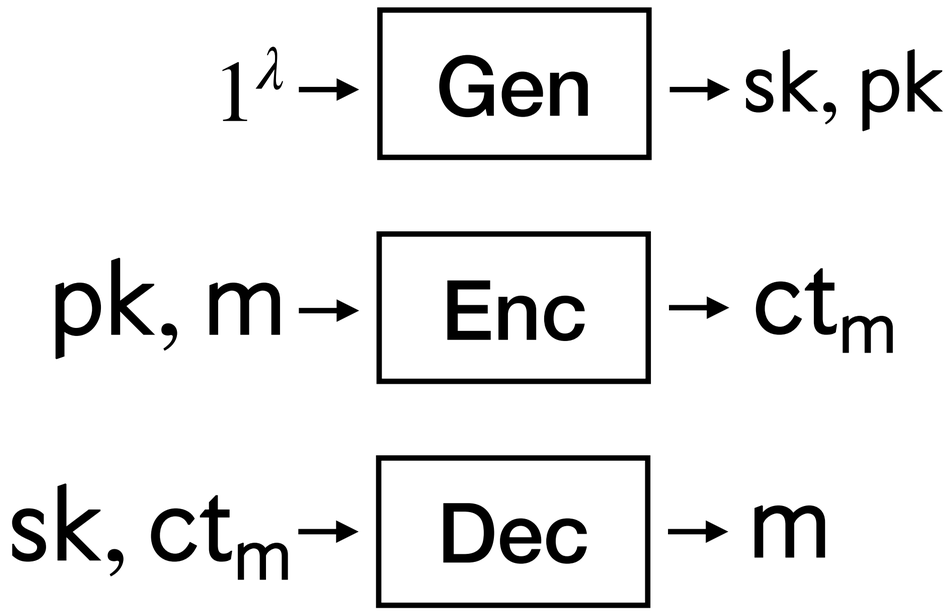
Impossibility of Strong KDM Security with Auxiliary Input

Cody Freitag[1], Ilan Komargodski[2], Rafael Pass[1]

[1]Cornell Tech [2]NTT Research, Hebrew University

Public-Key Encryption

Syntax



Semantic Security

$$ct_0 \approx ct_1$$

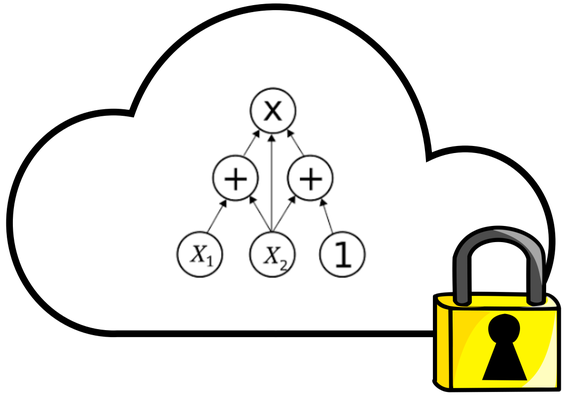
Fix messages, then probability is over a random sk, pk.

What if the message depends on the keys?

Disk Encryption

Circular Security

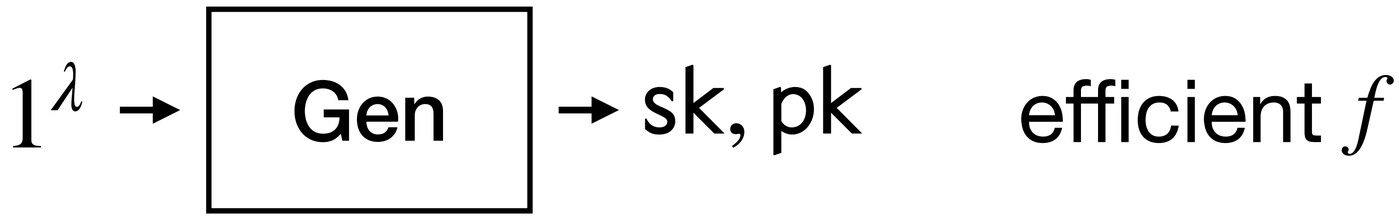
$1^{\lambda} \rightarrow$ **Gen** $\rightarrow$ sk, pk



Fully Homomorphic Encryption

$$ct_{0^s} \approx ct_{sk}$$

Key-Dependent Message Security



$$\mathsf{ct}_{0^s} \approx \mathsf{ct}_{f(\mathsf{sk})}$$

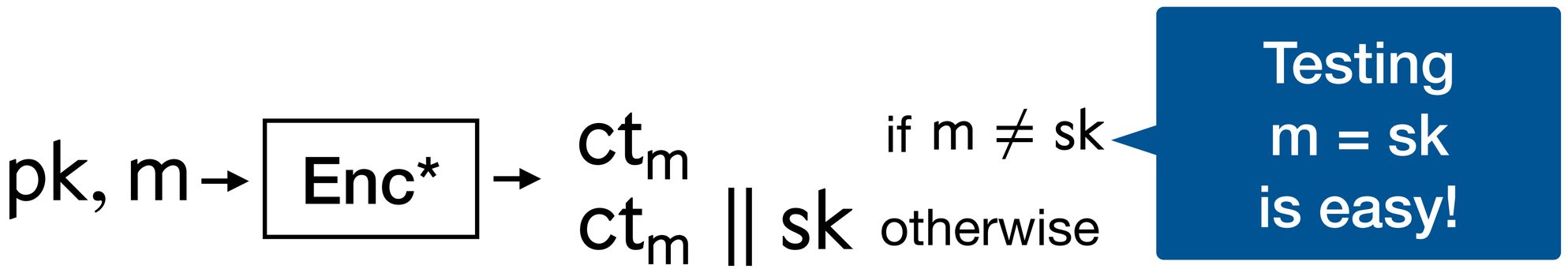
Messages depend (polynomially) on the keys

Is Every Semantically Secure Scheme also KDM Secure?

NO!

There exists an encryption scheme such that

$$ct_0 \approx ct_1 \quad \text{but} \quad ct_{0^s} \not\approx ct_{sk}$$



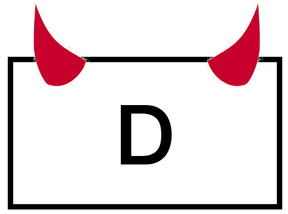
Does not imply *every* scheme does not satisfy KDM security!

- KDM security in ROM [BRS ’02]

- “Bounded” KDM from various structured assumptions
  - e.g. DDH, LWE, QR [BHHO ’08, BHHI ’09, ACPS ’09, BG ’10, A ’11]
- In fact, most “natural” schemes are ***believed to be*** KDM secure

Strong KDM Security with Auxiliary Input

1

For all $1^\lambda \rightarrow$  $\rightarrow \mathsf{pk}, z$ and inefficient f

3

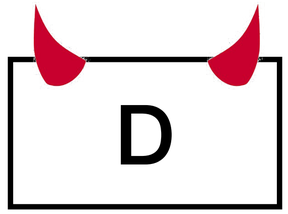
$$z, \mathsf{ct}_0 \approx z, \mathsf{ct}_1 \Rightarrow z, \mathsf{ct}_{0^s} \approx z, \mathsf{ct}_{f(\mathsf{pk},z)}$$

2

Strengthenings

1. Possibly malicious generation of keys
2. Additional public auxiliary input — for use inside another protocol
3. KDM security to hold even for exponential time functions

Strong KDM Security with Auxiliary Input

For all $1^\lambda \rightarrow$  $\rightarrow \mathsf{pk}, z$ and inefficient f

$$z, \mathsf{ct}_0 \approx z, \mathsf{ct}_1 \Rightarrow z, \mathsf{ct}_{0^s} \approx z, \mathsf{ct}_{f(\mathsf{pk},z)}$$

Used to construct 2-message witness hiding protocols [DK18]

In isolation, none of the modifications seem harmful.

Does there *exist* such a scheme?

Main Result: NO!

Assuming **LWE** and **one-way permutations**,
no (semantically secure) encryption scheme satisfies
strong KDM security with auxiliary input.

Even with short aux. input
(assuming non-leveled FHE)

Outline of Proof

Let (Gen, Enc, Dec) be ***any*** secure encryption scheme.

We construct a distribution D and a function f such that

A $z, \mathsf{ct}_0 \approx z, \mathsf{ct}_1$ but B $z, \mathsf{ct}_{0^s} \not\approx z, \mathsf{ct}_{f(\mathsf{pk},z)}$

Two Ingredients

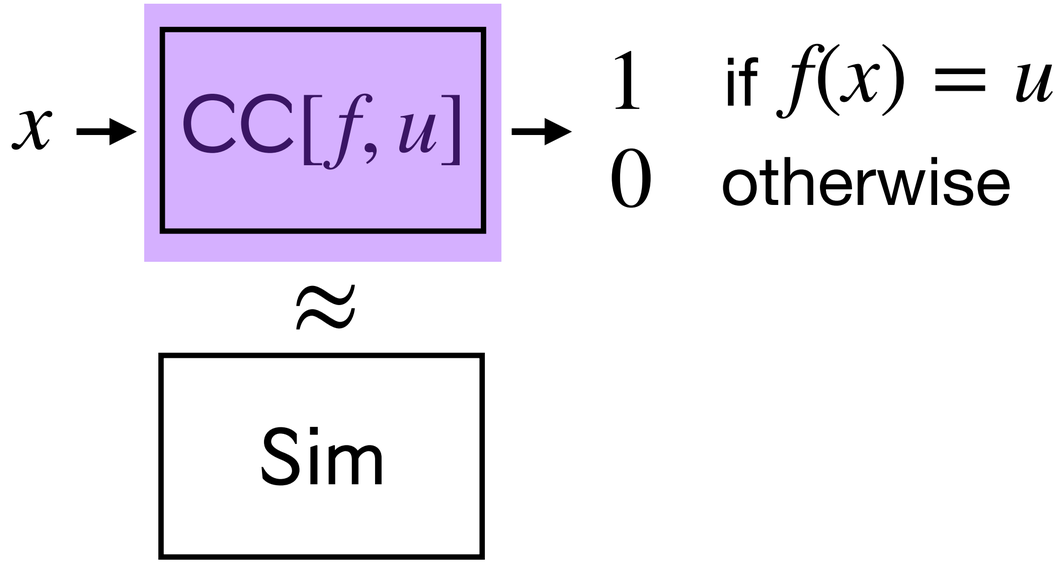
Specific pseudorandom generator

$$G(s) \mapsto y_1, y_2$$

- y_2 determines y_1
- $y_1 \approx U_\lambda$ given y_2

exists from OWP [GL89]

Compute-and-compare obfuscation



exists from LWE [WZ17, GKW17]

Attack

Let (Gen, Enc, Dec) be ***any*** secure encryption scheme.

$D(1^\lambda)$:

$(y_1, y_2) \leftarrow G(U_\lambda)$

$(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen}(1^\lambda)$

$\widetilde{\mathsf{CC}} \leftarrow \boxed{\mathsf{CC}[\mathsf{Dec}_{\mathsf{sk}}, y_1]}$

Output $\mathsf{pk}, \left(y_2, \widetilde{\mathsf{CC}}\right)$

$f(\mathsf{pk}, (y_2, \widetilde{\mathsf{CC}}))$:

Output the value y_1 determined by y_2

Recall: Outline of Proof

Let (Gen, Enc, Dec) be ***any*** secure encryption scheme.

We construct a distribution D and a function f such that

A $z, \mathsf{ct}_0 \approx z, \mathsf{ct}_1$ but B $z, \mathsf{ct}_{0^s} \not\approx z, \mathsf{ct}_{f(\mathsf{pk},z)}$

B

$z, \mathsf{ct}_{0^s} \not\approx z, \mathsf{ct}_{f(\mathsf{pk},z)}$

Recall $z = \left(y_2, \widetilde{\mathsf{CC}}\right)$, $f(\mathsf{pk}, z) = y_1$, where $\widetilde{\mathsf{CC}} \leftarrow$ $\mathsf{CC}[\mathsf{Dec}_{\mathsf{sk}}, y_1]$

$A(z, \mathsf{ct}_\mathsf{m})$:

Output $\widetilde{\mathsf{CC}}(\mathsf{ct}_\mathsf{m})$

If $\mathsf{m} = 0^s$, $\mathsf{Dec}_{\mathsf{sk}}(\mathsf{ct}_{0^s}) \neq y_1$ w.h.p.

$\Rightarrow A(z, \mathsf{ct}_\mathsf{m}) = 0$

If $\mathsf{m} = y_1$, $\mathsf{Dec}_{\mathsf{sk}}(\mathsf{ct}_{y_1}) = y_1$

$\Rightarrow A(z, \mathsf{ct}_\mathsf{m}) = 1$

Outline of Proof

Let (Gen, Enc, Dec) be ***any*** secure encryption scheme.

We construct a distribution D and a function f such that

A $z, \mathsf{ct}_0 \approx z, \mathsf{ct}_1$ but B $z, \mathsf{ct}_{0^s} \not\approx z, \mathsf{ct}_{f(\mathsf{pk},z)}$

A

$z, \mathsf{ct}_0 \approx z, \mathsf{ct}_1$

Hybrid 0: $A(z, \mathsf{ct}_0)$ using D

$D(1^\lambda)$:

$(y_1, y_2) \leftarrow G(U_\lambda)$

$(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen}(1^\lambda)$

$\widetilde{\mathsf{CC}} \leftarrow \mathsf{CC}[\mathsf{Dec}_{\mathsf{sk}}, y_1]$

Output $\mathsf{pk}, \left(y_2, \widetilde{\mathsf{CC}}\right)$

A

$z, \mathsf{ct}_0 \approx z, \mathsf{ct}_1$

Hybrid 0: $A(z, \mathsf{ct}_0)$ using D

Hybrid 1: $A(z, \mathsf{ct}_0)$ using D_{sim}

Hybrid 2: $A(z, \mathsf{ct}_1)$ using D_{sim}

$D_{\mathsf{sim}}(1^\lambda)$:

$(y_1, y_2) \leftarrow G(U_\lambda)$

$(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen}(1^\lambda)$

$\widetilde{\mathsf{CC}} \leftarrow$ Sim

t pk, $\left(y_2, \widetilde{\mathsf{CC}}\right)$

Requires y_1 has pseudo-entropy given y_2.

A

$z, \mathsf{ct}_0 \approx z, \mathsf{ct}_1$

Hybrid 0: $A(z, \mathsf{ct}_0)$ using D

Hybrid 1: $A(z, \mathsf{ct}_0)$ using D_{sim}

Hybrid 2: $A(z, \mathsf{ct}_1)$ using D_{sim}

Hybrid 3: $A(z, \mathsf{ct}_1)$ using D

$D(1^\lambda)$:

$(y_1, y_2) \leftarrow G(U_\lambda)$

$(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen}(1^\lambda)$

$\widetilde{\mathsf{CC}} \leftarrow \mathsf{CC}[\mathsf{Dec}_{\mathsf{sk}}, y_1]$

Output $\mathsf{pk}, \left(y_2, \widetilde{\mathsf{CC}}\right)$

Outline of Proof

Let (Gen, Enc, Dec) be ***any*** secure encryption scheme.

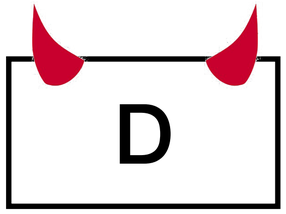
We construct a distribution D and a function f such that

A $z, \mathsf{ct}_0 \approx z, \mathsf{ct}_1$

but

B $z, \mathsf{ct}_{0^s} \not\approx z, \mathsf{ct}_{f(\mathsf{pk},z)}$

Yeah, but what if the auxiliary input is really short?

For all $1^\lambda \to$  $\to \mathsf{pk}, z$ and inefficient f

$$z, \mathsf{ct}_0 \approx z, \mathsf{ct}_1 \Rightarrow z, \mathsf{ct}_{0^s} \approx z, \mathsf{ct}_{f(\mathsf{pk},z)}$$

whenever $|z| \ll |\mathsf{pk}|$

- Still can be used for 2-message witness hiding [DK18]

Still no…

Key idea: maliciously generate sk, pk using a short seed!

- Can make y_1, y_2 much shorter than pk.
- Can compress description of $\mathsf{Dec}_{\mathsf{sk}}$ and hence $\widetilde{\mathsf{CC}}$.

Requires succinct compute-and-compare obfuscation

exists from non-leveled FHE [WZ17]

Takeaways

KDM security can
be really useful!

but be careful to
push it too far…

In natural scenarios, “weak” forms of obfuscation can be used to break security.