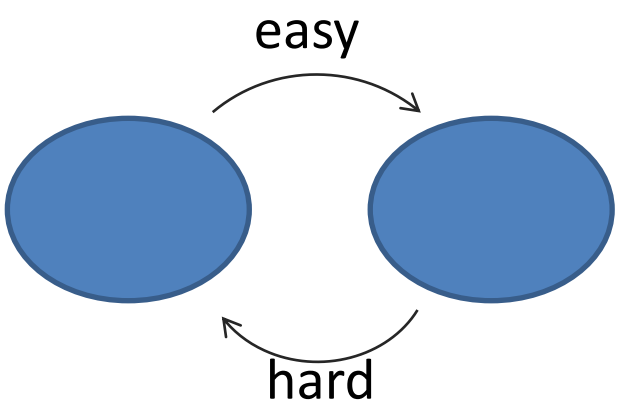
On cryptographic (r)evolutions
– from MiniCrypt to Obfustopia –

Christopher Brzuska
chris.brzuska@aalto.fi

Aalto University, Finland

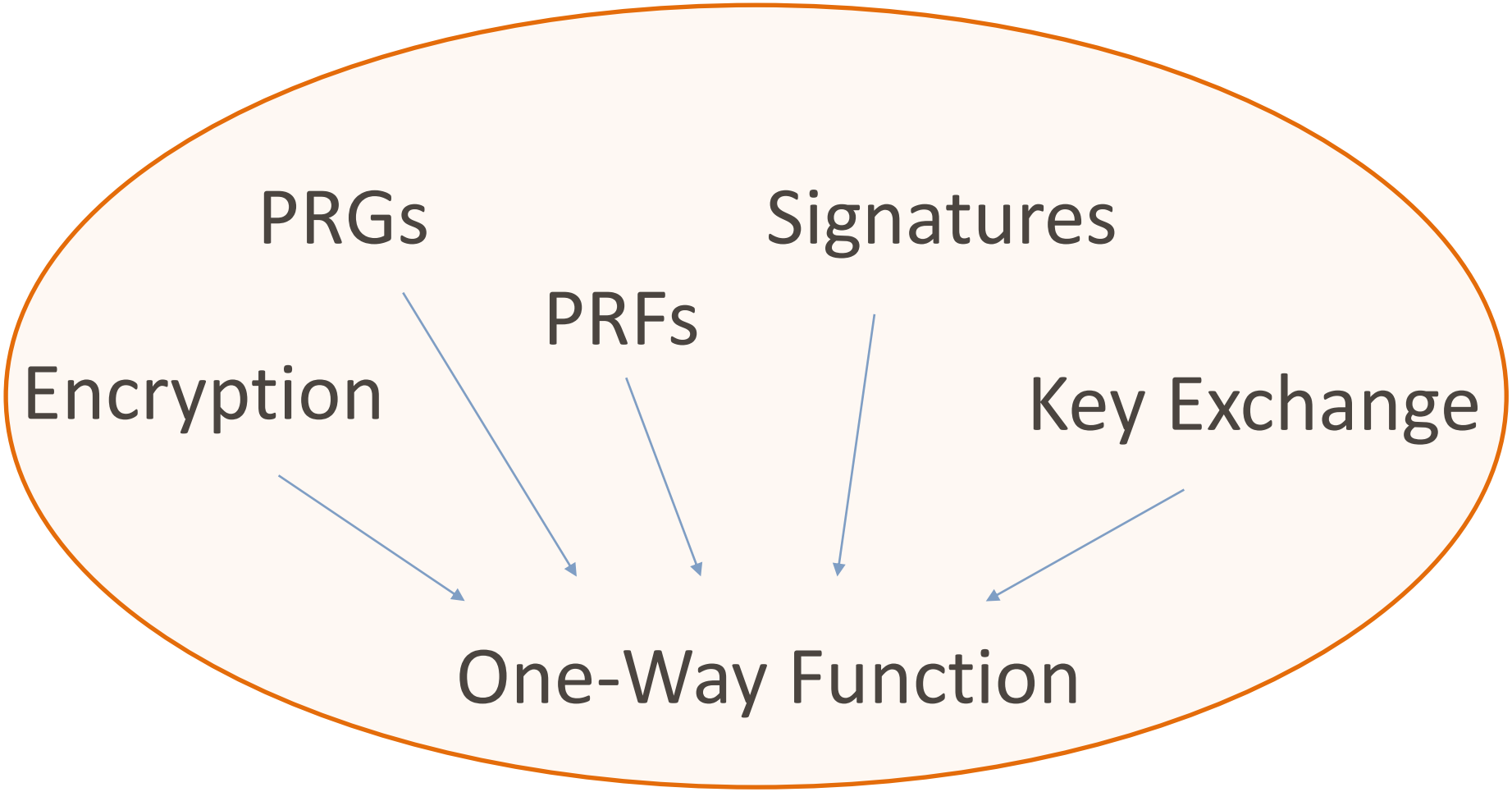
Recall crypto facts

One-Way Function (OWF)



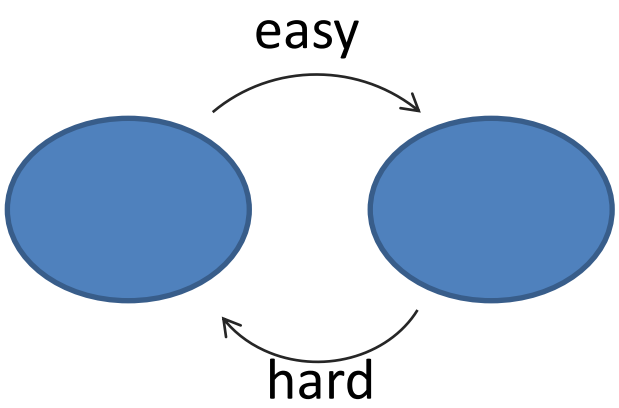
Impagliazzo-Luby

My interpretation:
No One-Way Function, no crypto
No One-Way Function, I need a new job.



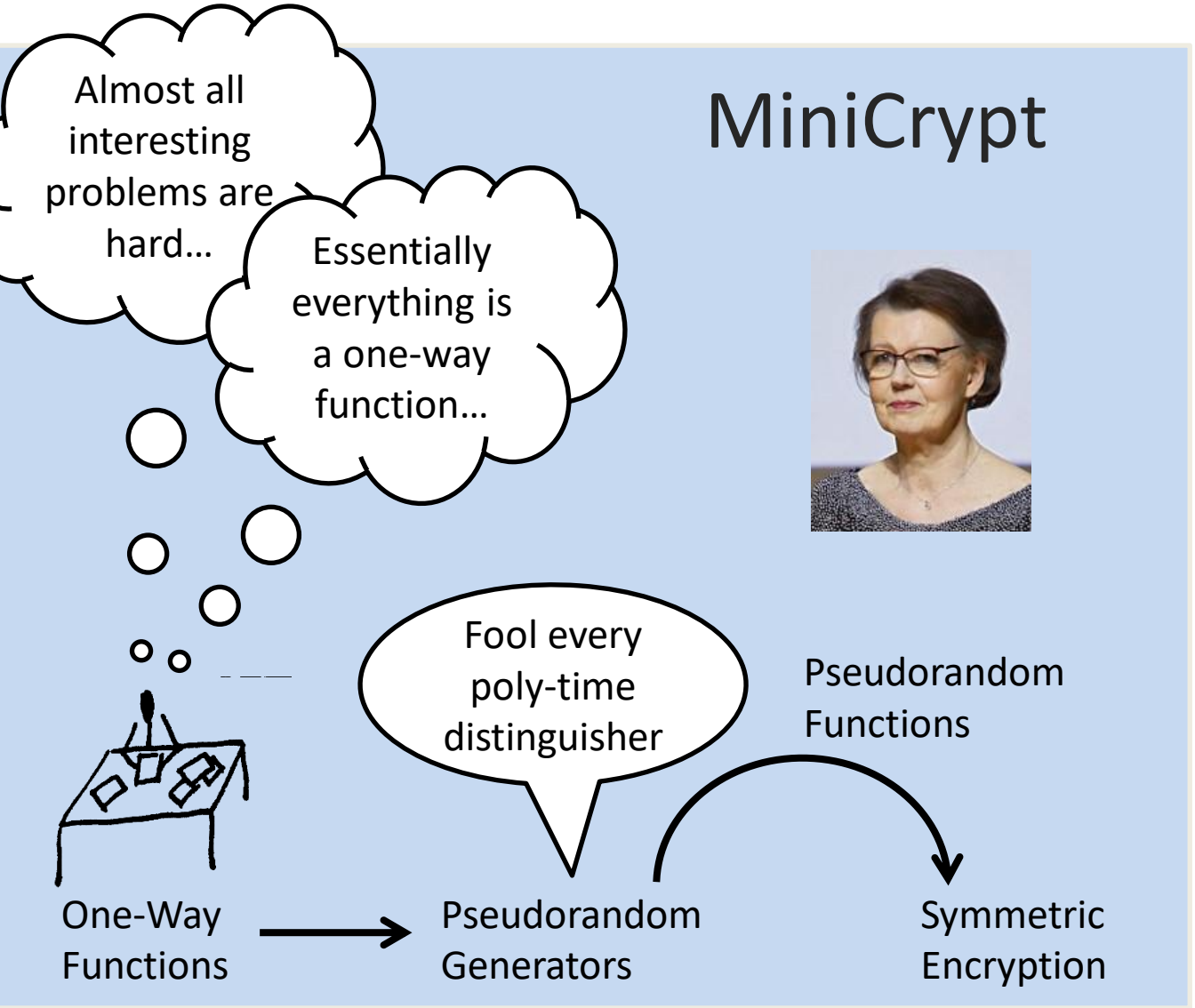
Recall crypto facts

One-Way Function (OWF)



1. OWF => NP≠P known
   NP≠P => OWF OPEN
2. “Everything“ in crypto implies
   implies OWFs

The cryptographic (r)evolution(s)



Impagliazzo's "worlds"

reasoneable

Almost all interesting problems are hard…

Essentially everything is a one-way function…

MiniCrypt

Cryptomania

Fool every poly-time distinguisher

Pseudorandom Functions

One-Way Functions → Pseudorandom Generators → Symmetric Encryption

Trapdoor Functions

Impagliazzo‘s “worlds“

MiniCrypt

Symmetric Encryption

Pseudorandom Functions

Pseudorandom Generators

One-Way Functions

Cryptomania (1976)

Trapdoor Functions

Fully Homo-morphic Encryption (2009)

Obfus-topia (2013)

Indistinguishability Obfuscation (iO)

Gilad Asharov
at Eurocrypt 2015 Rump Session

We can build everything from iO…

Perhaps, iO is Crypto-complete?

Gilad Asharov
at Eurocrypt 2015 Rump Session

We can build everything from iO…

Perhaps, iO is CRYPTO-complete?

Gilad Asharov and Gil Segev show that at least, iO is not Crypto-complete. ☺

[AS15]: Asharov-Segev, Limits on the Power of iO and Functional Encryption. FOCS 2015

[BB16]: Asharov-Segev, On Constructing One-Way Permutations from iO. TCC 2016-A

We have fantastic applications of iO!

…but this is not, what this talk is about.

This talk is about:

iO as a foundational (& weird!) concept.

Odd Facts about indistinguishability Obfuscation (iO)

1. iO does *not* imply One-Way Functions.

necessarily

necessarily

It suffices, if I show you
a proof of the third statement.
Then 1. and 2. follow as well.

Obfuscation

same functionality
hides structure

Program C(.) $\xrightarrow{\text{Obf}}$ C‘(.)

Think of C(.) as a circuit with OR and NAND gates.

Or… …think of C as a C-program and C‘ as an unreadable version of it…

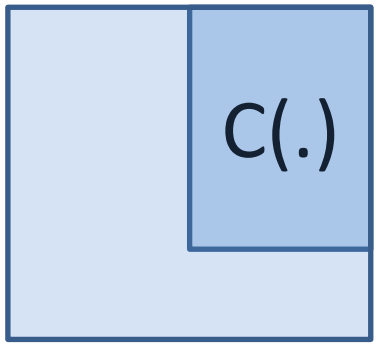
even worse
than before.

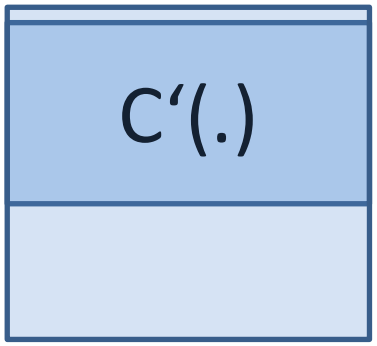
…and we want to <u>prove</u> that the obfuscation is “secure“.

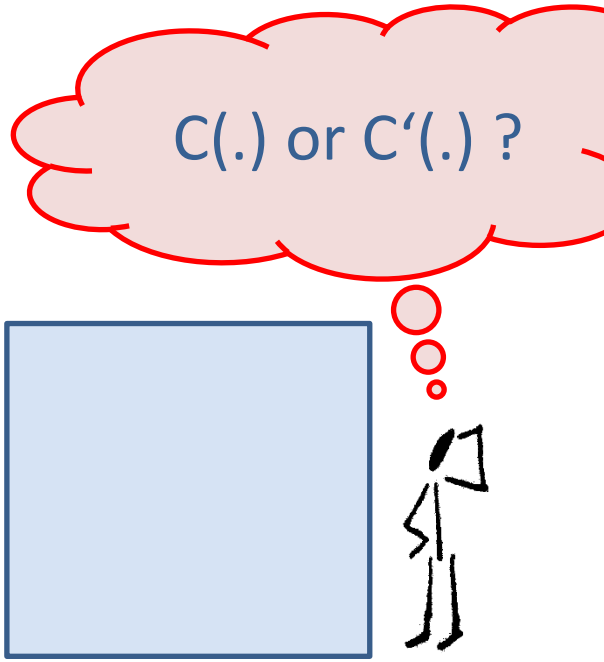
Indistinguishability Obfuscation iO

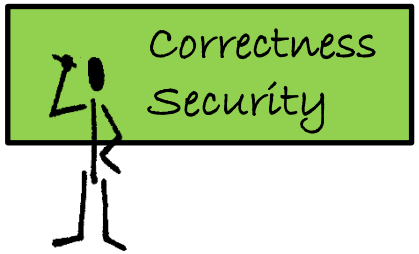
- For all* circuits C, C‘ that compute the same function:

iO(C(.)) and iO(C‘(.)) are indistinguishable.









*of roughly the same size.

If P=NP, iO exists.

efficient

Construction: Obf(C):=

lexicographically first circuit that computes the same function as C.

Security Proof: Take circuits C(.) and C'(.) that computer the same function.

Need to show: Obf(C(.)) ≈Obf(C'(.))

Why do Obf(C(.)) and Obf(C'(.)) look similar?

Odd Facts about indistinguishability Obfuscation (iO)

1. iO does *not* imply One-Way Functions.
2. iO does not imply that P ≠ NP.
3. If P=NP, then iO exists!

Options for the rest of the talk:

i. Prove 4a. (quite easy)
ii. Prove 4b. (main technique, not today)
iii. Discuss what we know about the existence of statistical iO (without proofs)
iv. Discuss 5.

---

4. iO with *statistical* security (no assumptions) might exist. If it does, then
   a. NP≠P => OWFs
   b. OWFs => Public-key encryption
5. iO is mutually exclusive with other assumptions that were believed before.

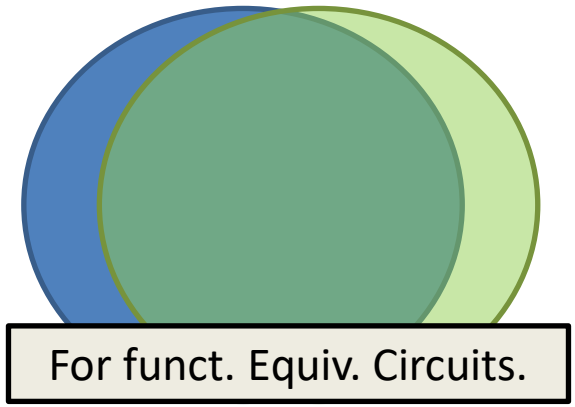
Indistinguishability Obfuscation with statistical security siO

- **Correctness**: iO(C(.)) and C(.) compute the same function.

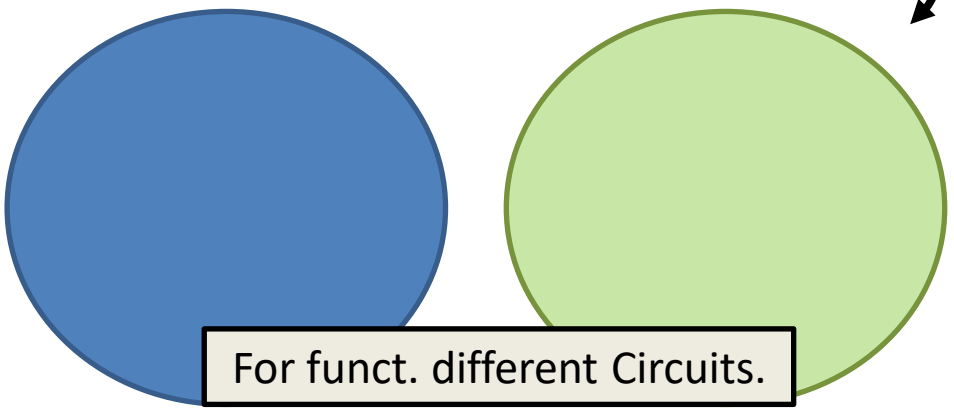
*of roughly the same size.

- **Security:** For all* C, C‘ that compute the same function:

  iO(C(.)) and iO(C‘(.)) are statistically close distributions



For funct. Equiv. Circuits.



For funct. different Circuits.

NP≠P => OWFs

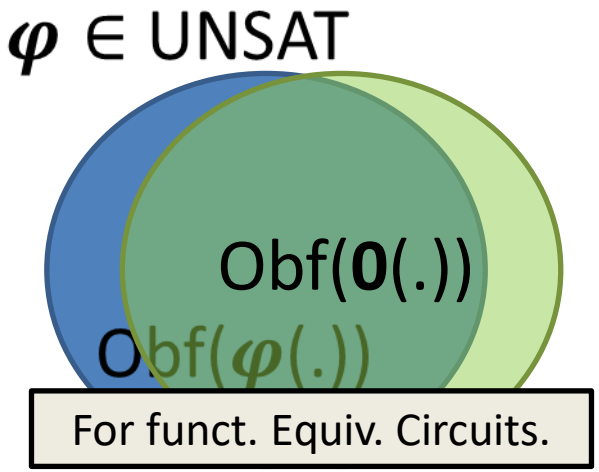
$r \rightarrow \text{Obf}(\mathbf{0}(.);r)$

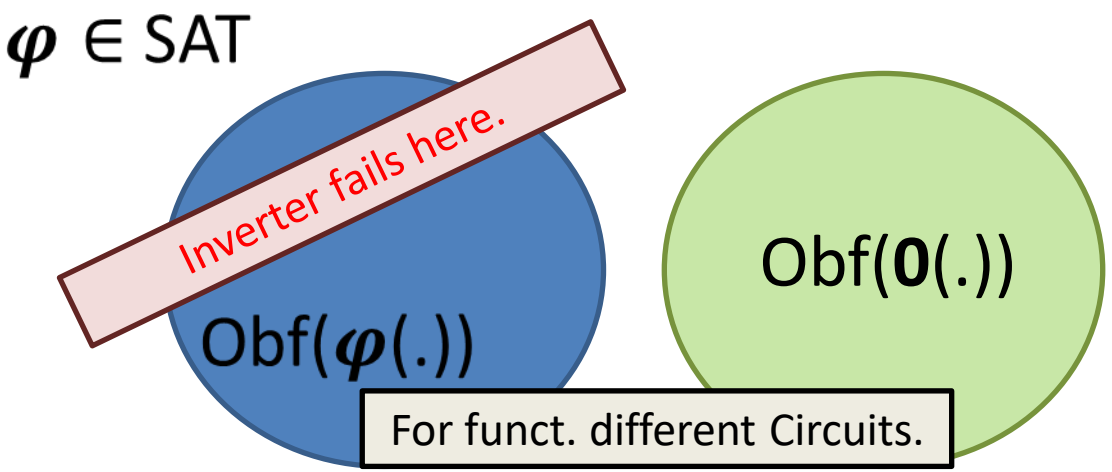
Constant zero Circuit that maps all values to 0.

Randomness of the obfuscator

Why is this an OWF?

Assume towards contradiction that there exists an inverter…
Goal: distinguish satisfiable from unsatisfiable formulae (& reach contradiction)





Options for the rest of the talk:

i. Prove 4a. **Done.**
ii. Prove 4b. (main technique, not today)
iii. Discuss what we know about the existence of statistical iO (without proofs)
iv. Discuss 5.

---

4. iO with *statistical* security (no assumptions) might exist. If it does, then
   a. NP≠P => OWFs
   b. OWFs => Public-key encryption
5. iO is mutually exclusive with other assumptions that were believed before.

Options for the rest of the talk:

i. Prove 4a. **Done.**
ii. Prove 4b. (main technique, not today) **Skipped.**
iii. Discuss what we know about the existence of statistical iO (without proofs)
iv. Discuss 5.

---

4. iO with *statistical* security (no assumptions) might exist. If it does, then
   a. NP≠P => OWFs
   b. OWFs => Public-key encryption
5. iO is mutually exclusive with other assumptions that were believed before.

Options for the rest of the talk:

i. Prove 4a. **Done.**
ii. Prove 4b. (main technique, not today) **Skipped.**
iii. Discuss what we know about the existence of statistical iO (without proofs) **Now.**
iv. Discuss 5.

---

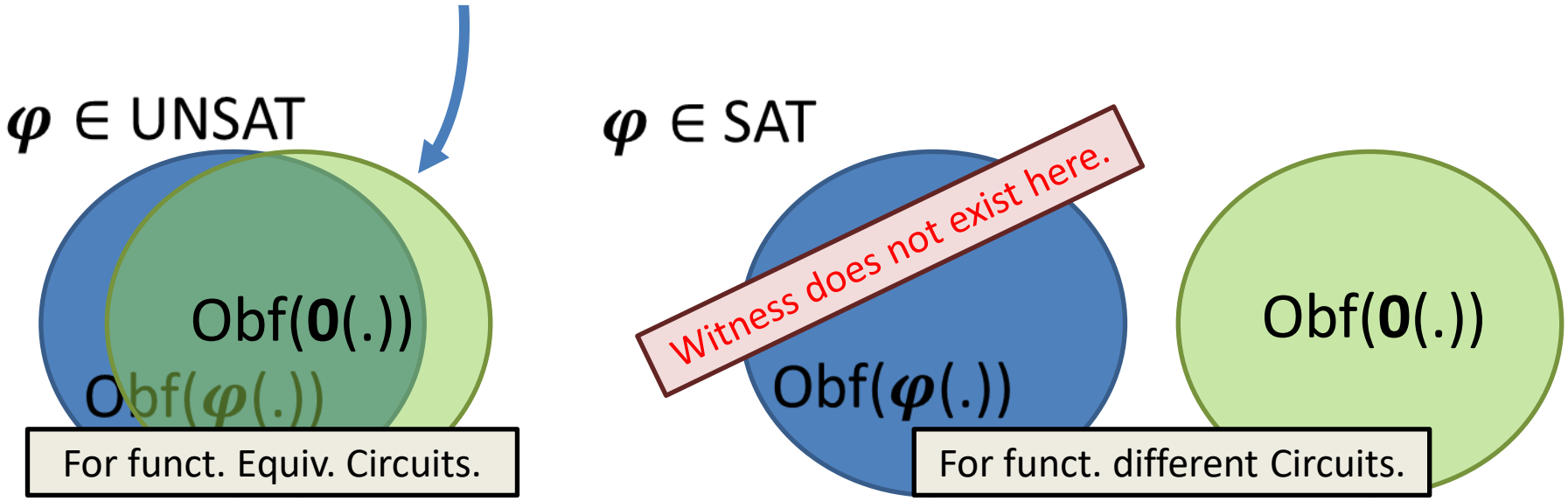
4. iO with *statistical* security (no assumptions) might exist. If it does, then
   a. NP≠P => OWFs
   b. OWFs => Public-key encryption
5. iO is mutually exclusive with other assumptions that were believed before.

Eierlegende Wollmilchsau

(egg-laying wool milk pig)

iO with statistical security does not exist (unless coNP ⊆NP)

- ∃ siO ⇒ coNP ⊆ NP

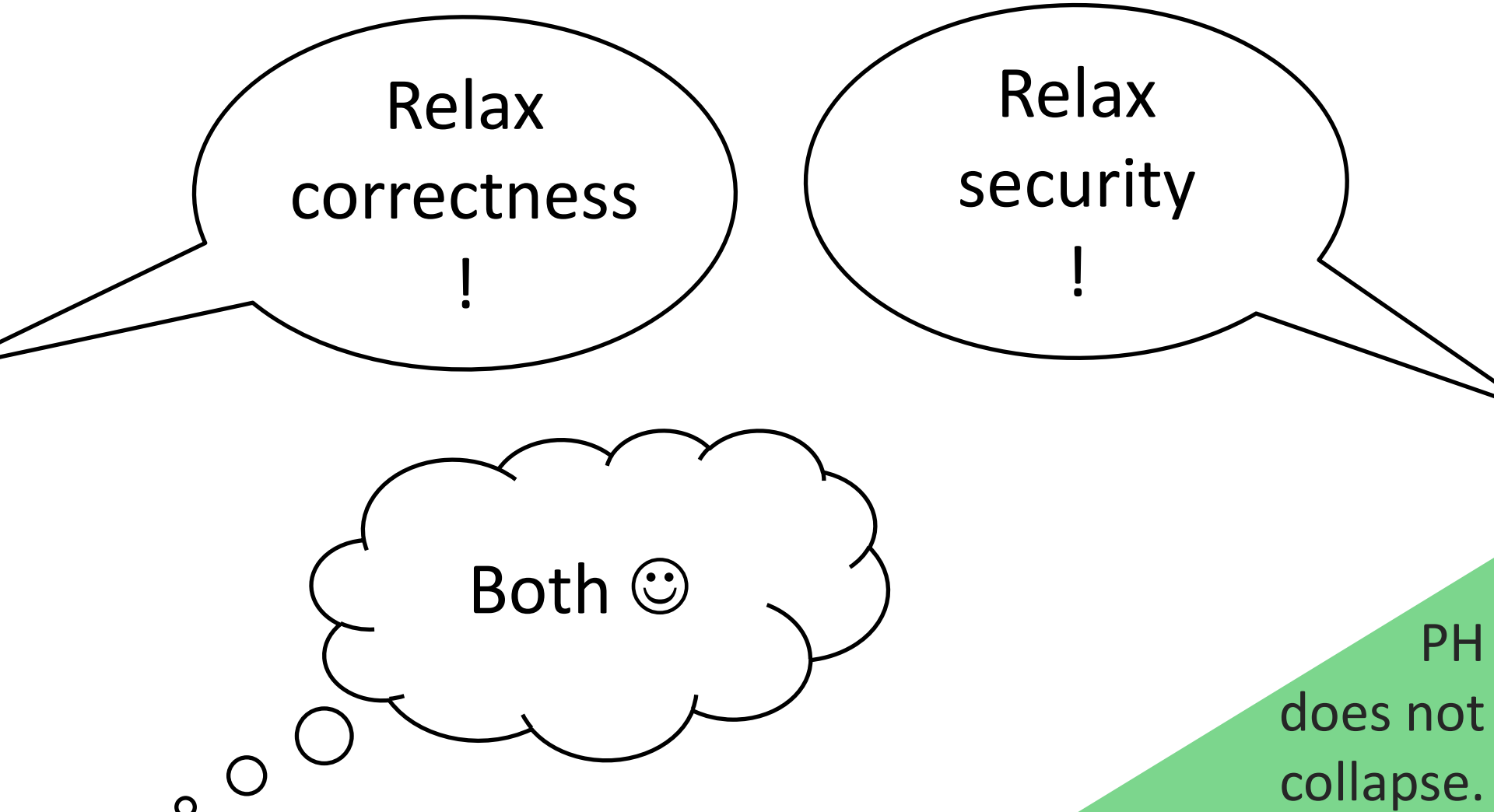


[GR05]: iO with statistical security does not exist.

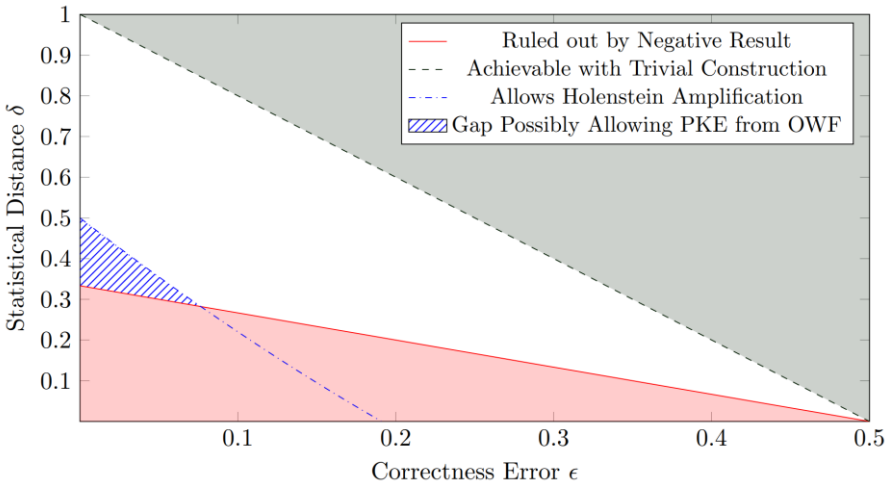
Let‘s be less ambitious.

PH does not collapse.

[GR05]: iO with statistical security does not exist.



iO with statistical $(1-\delta)$ security $(1-\epsilon)$ correctness



Impossible (OWF, PH): $2\varepsilon < 1 - 3\delta$

OWFs exist

PH does not collapse.

[BBF16]: Brakerski-Brzuska-Fleischhacker: On Stat. Sec. Obf. with Approx. Correctness, CRYPTO 16

Options for the rest of the talk:

i. Prove 4a. **Done.**
ii. Prove 4b. (main technique, not today) **Skipped.**
iii. Discuss what we know about the existence of statistical iO (without proofs) **Done.**
iv. Discuss 5 (main technique, not today) **Now.**

---

4. iO with *statistical* security (no assumptions) might exist. If it does, then
   a. NP≠P => OWFs
   b. OWFs => Public-key encryption
5. iO is mutually exclusive with other assumptions that were believed before.

Point function obfuscation

Point function: $p_{x,y}(x') := \begin{cases} \textbf{if } x=x' \text{ return } y \\ \textbf{else} \quad \text{return } 0 \end{cases}$

$\xrightarrow{\$}$ x, y

x needs to have high entropy

Else, the sampler could choose

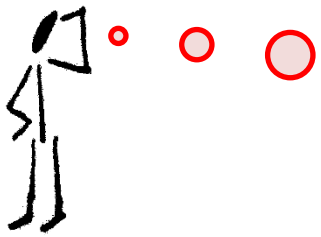
x=0…0 y=1..1

And the distinguisher could check

p(0..0)=1..1

b=0: p:=PointObf($p_{x,y}$(.)) ✓

b=1: p:=PointObf($p_{a,b}$(.)) for **random** a, b ✗



Get p.

Real p or random p?

Point function obf. w. leakage [BM14]

Point function: $p_{x,y}(x') := \begin{cases} \textbf{if } x=x' \text{ return } y \\ \textbf{else} \quad \text{return } 0 \end{cases}$

$\xrightarrow{\$}$ x, y, **leak**

x needs to have high entropy given **leak**

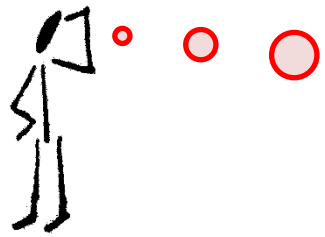
circuit iO(C[x,z]), z:= PRG(y)

C[x,z](p):
if PRG(p(x))=z **ret** x
return 0

b=0: p:=PointObf($p_{x,y}$(.)) ✓

b=1: p:=PointObf($p_{a,b}$(.)) for **random** a, b ✗

Get p
and leak.



Real p or random p?

Point function obf. w. leakage [BM14]

Point function: $p_{x,y}(x') := \begin{cases} \textbf{if } x=x' \text{ return } y \\ \textbf{else} \quad \text{return } 0 \end{cases}$

$\xrightarrow{\$}$ x, y, **leak**

x needs to have high entropy given **leak**

uniformly random

circuit iO(C[x,z]), z:= ~~PRG(y)~~

C[~~x,z~~](p):

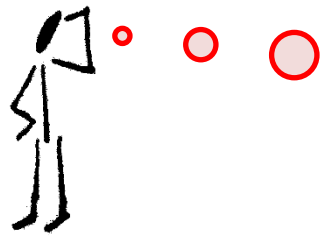
~~**if** PRG(p(x))=z **ret** x~~

return 0

b=0: p:=PointObf($p_{x,y}$(.)) ✓

b=1: p:=PointObf($p_{a,b}$(.)) for **random** a, b ✗

Get p **and leak.**



Real p or random p?

Point function obf. w. leakage [BM14]

Point function: $p_{x,y}(x') := \begin{cases} \textbf{if } x=x' \text{ return } y \\ \textbf{else} \quad \text{return } 0 \end{cases}$

$\xrightarrow{\$}$ x, y, **leak**

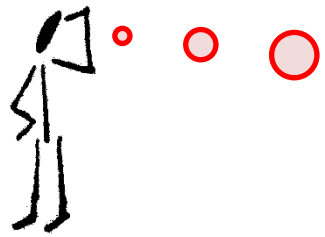
x needs to have high entropy given **leak**

Secure point function with leakage does not exist if iO + PRG exist.

b=0: p:=PointObf($p_{x,y}$(.))

b=1: p:=PointObf($p_{a,b}$(.)) for **random** a, b

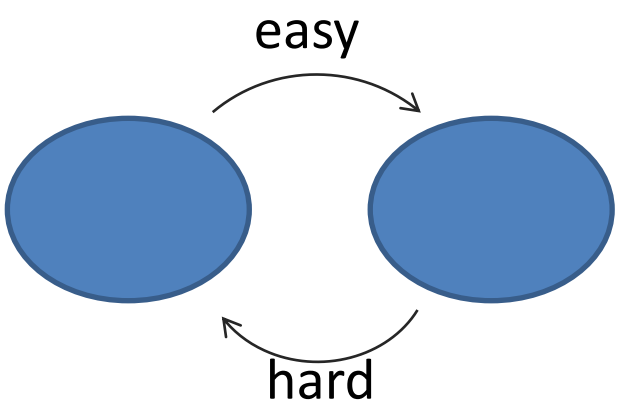
Get p **and leak.**



Real p or random p?

Recall crypto facts

One-Way Function (OWF)



1. OWF => NP≠P known
   NP≠P => OWF OPEN
2. "Everything" in crypto implies
   implies OWFs
3. Build public-key encryption from OWF? OPEN

Odd Facts about indistinguishability Obfuscation (iO)

1. iO does *not* imply One-Way Functions.
2. iO does not imply that P ≠ NP.
3. If P=NP, then iO exists!
4. iO with *statistical* security might exist. If it does, then
   a. NP≠P => OWFs
   b. OWFs => Public-key encryption
5. iO is mutually exclusive with other assumptions that were believed before.

but under reasoneable assumptions (OWF, coNP ⊄ NP), it doesn't.

Some iO references and topics you can ask me about ☺.

If you are interested to learn
more about crypto in general:
In autumn 2023, Russell and I teach
CS-E4340 Cryptography D together.
Welcome to join!

1. Main techniques:
   a) 0-circuit*
   b) puncturable PRFs*
   c) Complexity leveraging
2. Conceptually important implications & properties*
3. 2-out-of-1 results, 3-out-of-1 results for iO and its variants*: diO, siO*, saiO*, correctness issues
4. Positive results for XiO (subexp. complexity)
5. Construction stategies
   a. Low-degree multi-lin maps + low-depth PRG
   b. LWE → ask Russell Lai
6. Limits of the power of iO
7. Necessary assumptions for iO*
8. Applications
9. Relations to Functional Encryption

* = very easy for me
Purple = I know little.

Conceptually fundamental implications

positive

NP=P => iO exists: Reference? Folklore?

NP-hardness + iO => OWFs:

[KMNPRY14] Komargodski-Moran-Naor-Pass-Rosen-Yogev: OWFS & (Im)Perfect Obf., FOCS 14

OWFs + iO => PKE:

[SW14] Sahai-Waters: How to use iO: deniable encryption, and more, STOC 2014

PKE + iO => FHE:

[CLTV15] Canetti-Lin-Tessaro-Vaikuntanathan:

Obfuscation of probabilistic circuits and applications, TCC 15

https://www.youtube.com/watch?v=HWGNxUTrzC0

[CRRV17] Canetti-Raghuraman-Richelson-Vaikuntanathan: CCA-Secure FHE, PKC 2017

[BPR14] Bitansky-Paneth-Rosen, On the Cryptogr. Hardness of Finding a Nash Equilibrium, FOCS 14

https://www.youtube.com/watch?v=oEmcKBLu8pg

Further fundamental properties:

[GR07] Goldwasser-Rothblum: Ob Best-Possible Obfuscation, TCC 2007

„Classical“ negative result on obfuscation:

[BGIRSVY01] Barak-Goldreich-Impagliazzo-Rudich-Sahai-Vadhan-Yang,
On the (Im)possibility of Obfuscating Programs. CRYPTO 2001

iO is mutually exclusive with… 2-out-of-1 and 3-out-of-1 results:

[BCPR14] Bitansky-Canetti-Paneth-Rosen, On the existence of extractable OWFs, STOC 14

[BCCGKPR14] Bitansky-Canetti-Cohn-Goldwasser-Kalai-Paneth-Rosen:
On the impossibility of obfuscation with auxiliary input or a universal simulators, CRYPTO 14

[BFM14] Brzuska-Farshim-Mittelbach: Indistinguishability Obfuscation and UCEs, CRYPTO 14

[BM14] Brzuska-Mittelbach: iO vs. Multi-Bit Point Obfuscation, ASIACRYPT 2014

[BFM15] Brzuska-Farshim-Mittelbach: Random Oracle Uninstantiability from iO, TCC 15

[Kom16] Komargodski: Leakage Resilient OWF: The Auxiliary-input Setting, TCC 2016-B

[BST16] Bellare-Stepanovs-Tessaro: Contention in Cryptoland: Obf., Leakage & UCE, TCC 16-A

[BS16] Bellare-Stepanovs: Point-Function Obf.: A Framework and Generic Constructions, TCC 16-A

…essentially, all works use the same technique and break 2-stage adversaries ☺

Differing-inputs obfuscation (diO) is mutually exclusive with… 2-out-of-1 and 3-out-of-1 results:

[BSW17] Bellare-Stepanovs-Waters: New Negative Results on diO, EC 17

[GGHW14] Garg-Gentry-Halevi-Wichs:
On the Implausibility of diO & Extractable Witness Encryption with Auxiliary Input, CRYPTO 14

negative

Statistically secure iO is mutually exclusive with… 2-out-of-1 results:

[GR07] Goldwasser-Rothblum: On best-possible obfuscation, TCC 07

[BBF16] Brakerski-Brzuska-Fleischhacker: On Stat. Sec. Obf. with Approx. Correctness, CRYPTO 16

(The negative result leaves a gap ☺)

positive

Obfuscators/Witness Encryption (WE) with non-trivial efficiency (XiO – x for exponential)

[LPST16] Lin-Pass-Seth-Telang: iO with non-trivial efficiency, PKC 16

[BJKPW17]: Brakerski-Jain-Komargodski-Passelègue-Wichs:
Non-Trivial WE & Null-iO from Standard Assumptions, ePrint 2017

clarifying

On the role of correctness questions:

[BBF16]: Brakerski-Brzuska-Fleischhacker: On Stat. Sec. Obf. with Approx. Correctness, CRYPTO 16

[BV17] Bitansky-Vaikuntanathan: A Note on Perfect Correctness by Derandomization, EC 2017

[BV17] Bitansky-Vaikuntanathan: iO: From approximate to exact, TCC 2016-A

[KMNPRY14] Komargodski-Moran-Naor-Pass-Rosen-Yogev: OWFS & (Im)Perfect Obf., FOCS 14

On the limits of iO:

[AS15]: Asharov-Segev: Limits on the Power of iO and Functional Encryption. FOCS 2015

[BB16]: Asharov-Segev: On Constructing One-Way Permutations from iO. TCC 2016-A

[AS16] Asharov-Segev: iO Does Not Reduce to Structured Languages. ePrint 2016

[BPW16] Bitansky-Paneth-Wichs:

Perfect Structure on the Edge of Chaos - TDPs from iO, TCC 2016-A

[BDV17] Bitansky-Degwekar-Vaikuntanathan:

Structure vs. Hardness Through the Obfuscation Lens. CRYPTO 2017

negative

Necessary assumptions for iO:

OWFs do not suffice:

[MMNRS16]: Mahmoody-Mohammed-Nematihaji-Pass-shelat:

Lower Bounds on Assumptions Behind Indistinguishability Obfuscation. TCC 16

Most recently: FHE, WE do not suffice:

[GMM17] Garg-Mahmoody-Mohammed: LBs on Obf. from All-or-Nothing Enc. Primitives. C 17

Constructing iO from LWE (most recent selection to my knowledge):

positive

[BJKPW17]: Brakerski-Jain-Komargodski-Passelègue-Wichs:
Non-Trivial WE & Null-iO from Standard Assumptions, ePrint 2017

[WZ17]: Wichs-Zirdelis: Obfuscating Compute-and-Compare Programs under LWE, ePrint 2017

[GKW17] Goyal-Koppula-Waters: Separating Semantic and Circular Security for Symmetric-Key Bit Encryption from the Learning with Errors Assumption. EC 17

[BVWW16] Brakerski-Vaikuntanathan-Wee-Wichs: Obf. Conj. under Entropic Ring LWE, ITCS 16

[BV16] Brakerski-Vaikuntanathan: Circuit-ABE from LWE: Unb. Attributes & Semi-adap. Sec. C 16

positive

The initial breakthrough construction:

[GGHRSW13]: Garg-Gentry-Halevi-Raykova-Sahai-Waters:
Candidate Indistinguishability Obfuscation and Functional Encryption for all Circuits. FOCS 13

Constructing iO from low-degree multi-linear encodings (most recent to my knowledge):

[Lin17] Huijia Lin: iO from SXDH on 5-Linear Maps and Locality-5 PRGs. CRYPTO 17

[LT17a] Lin-Tessaro: iO from Trilinear Maps and Block-Wise Local PRGs. CRYPTO 17

[LT17b] Lin-Tessaro: iO from Bilinear Maps and Block-Wise Local PRGs. ePrint 17

The assumptions in [LT17b] are broken, but the fixed ones are not ☺.

[AS17] Ananth-Sahai: Proj. Arithmetic Functional Encryption & iO from Degree-5 Mult Maps. EC17

Limits on low-degree PRGs (there is lots of related research on low-depth PRFs also…)

[BBKK17] Barak-Brakerski-Komarkodski-Kothari: Limits on Low-Degree Pseudorandom Generators
(Or: Sum-of-Squares Meets Program Obfuscation). ePrint 2017

[LV17] Lombardi-Vaikuntanathan:
On the Non-Existence of Blockwise 2-Local PRGs with Applications to iO. TCC 2017