CRYPTOGRAPHIC LOWER BOUNDS IN TFNP: RECENT ADVANCES

CHETHAN KAMATH
TEL AVIV UNIVERSITY

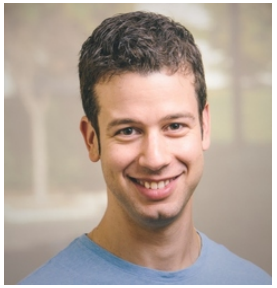
ADVANCES ON TOTAL SEARCH, ICALP 2022, JULY 4-TH

BASED ON:

[CHKPRRI9a,b]: CHOUDHURI, HUBÁČEK, PIETRZAK, ROSEN & G. ROTHBLUM







[BCHKLPR22]: BITANSKY, CHOUDHURI, HOLMGREN, LOMBARDI, PANETH & R. ROTHBLUM





LOWER BOUNDS FOR CLS FROM STD. ASSUMPTIONS

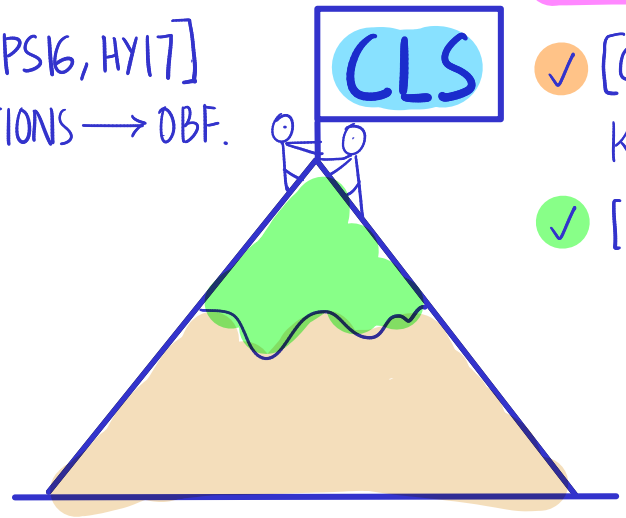
WELL-STUDIED, WEAK ASSUMPTIONS

DIFFERENT TECHNIQUES, ASSUMPTIONS

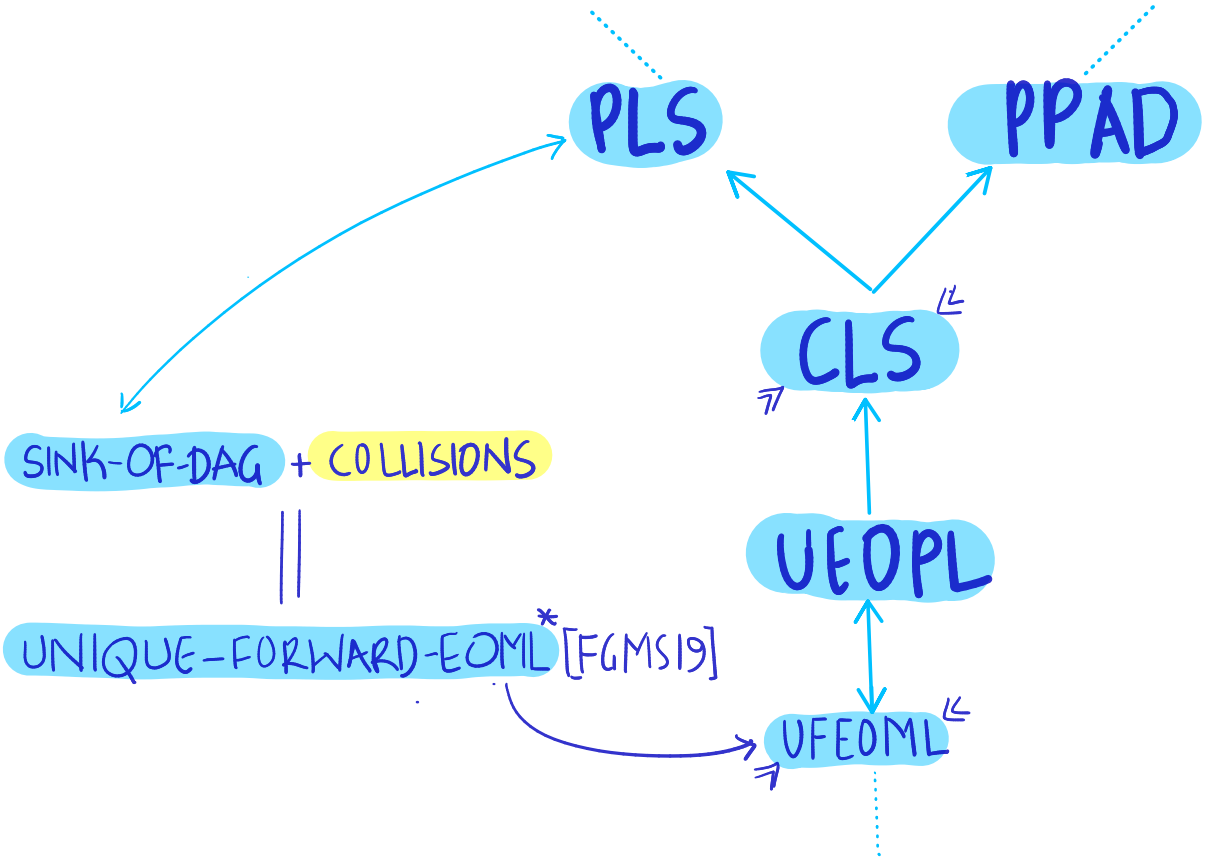
- "OBFUSTOPIA" APPROACH:
  1. OBFUSCATION → CLS
     - ✓ [BPR15, GPS16, HY17]
  2. STD. ASSUMPTIONS → OBF.
     - ✓ [JLS21]

- "PROOF SYSTEM" APPROACH:
  NON-INTERACTIVE PROOF → CLS
  - ✓ [CHKPRR19*, EFKM19, LV20, KPY20, JKKZ21]
  - ✓ [BCHKLPR22]

» THIS TALK «



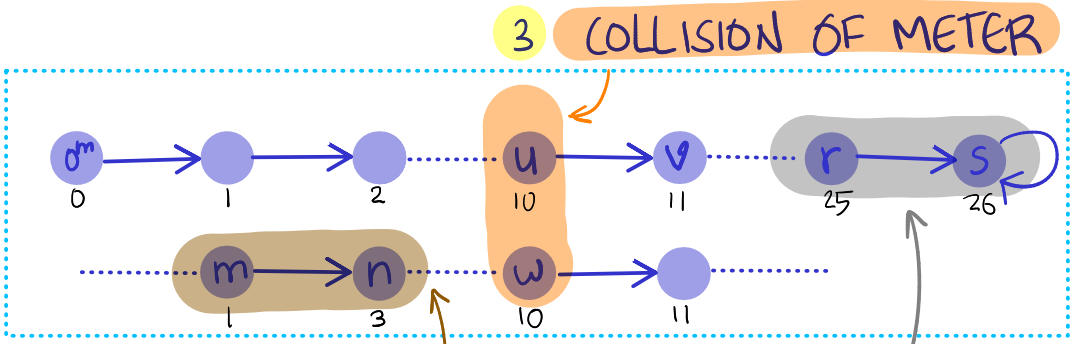
LOWER BOUNDS FOR CLS VIA UFEOML



*CALLED UNIQUE-FORWARD-EOPL+1 IN [FGMS19]

UNIQUE-FORWARD-EOML

- INPUT: SUCCESSOR & METER CIRCUITS



- SOLUTIONS 2 VIOLATION OF METER 1 SINK

UFEOML VIA PROOF SYSTEM APPROACH

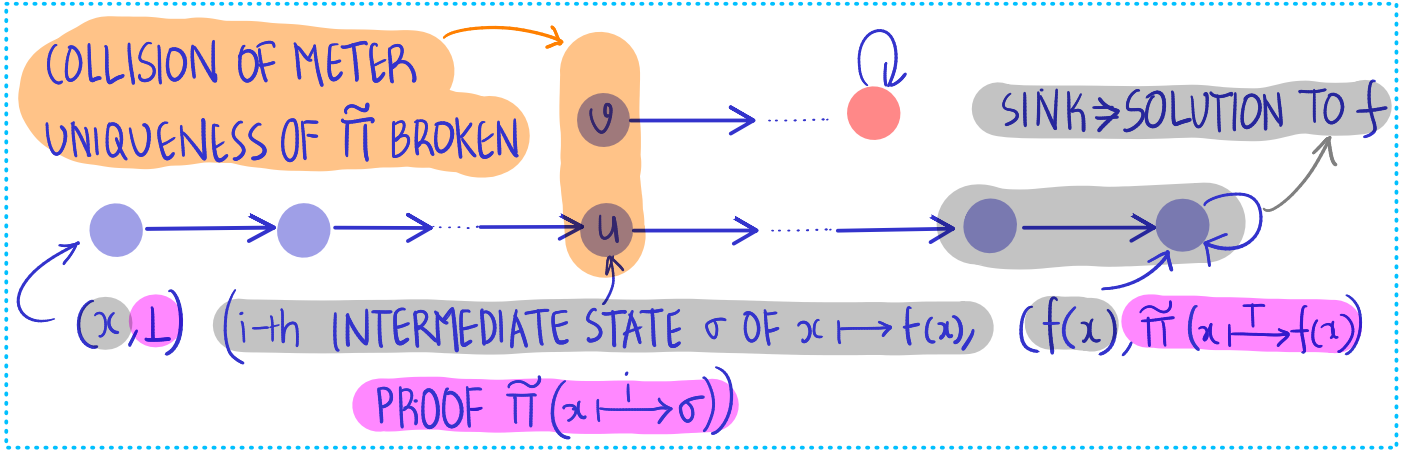
- GOAL: HARD DISTRIBUTION OF UFEOML

⇑

f(x) HARD-TO-COMPUTE & NON-INTERACTIVE PROOF $\widetilde{\Pi}$

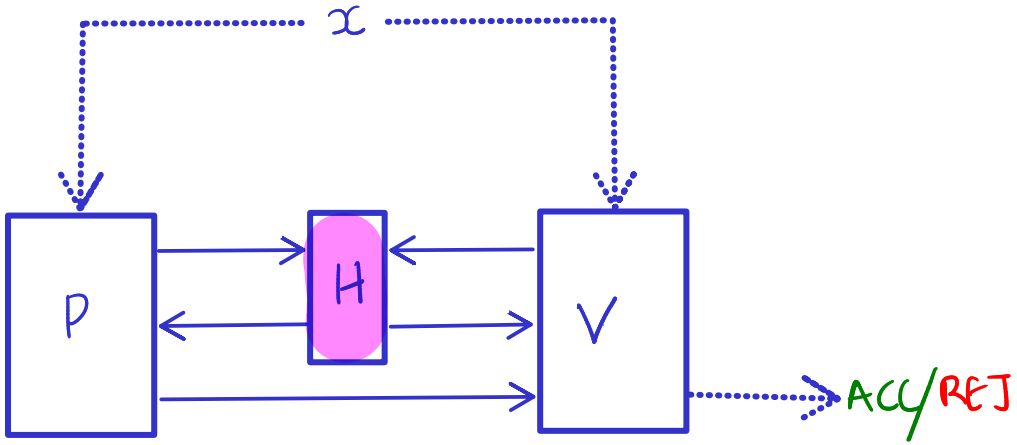
$d_f := \{(x,\sigma,i) : x \xmapsto{i \text{ STEPS}} \sigma\}$

1. SUCCESSOR REQUIRES "UPDATEABLE" $\widetilde{\Pi}$
2. HARDNESS REQUIRES "UNIQUE" $\widetilde{\Pi}$



UFEOML VIA FIAT-SHAMIR TRANSFORM

- NEW GOAL: UPDATEABLE & UNIQUE NON-INTERACTIVE PROOF $\widetilde{\Pi}$
- PUBLIC-COIN INTERACTIVE PROTOCOL $\xrightarrow{H}$ NON-INERACTIVE PROTOCOL
  - HASH FUNCTION



- FS TRANSFORM SOUND IF: Π IS SOUND $\Rightarrow$ $\widetilde{\Pi}$ IS SOUND

UFEOML VIA FIAT-SHAMIR TRANSFORM...

- NEW GOAL: UPDATEABLE & UNIQUE NON-INTERACTIVE PROOF $\widetilde{\Pi}$
- PUBLIC-COIN INTERACTIVE PROTOCOL $\xrightarrow{H}$ NON-INERACTIVE PROTOCOL
  - HASH FUNCTION

"COMPLEXITY PART"

- DESIGN INTERACTIVE PROTOCOL Π FOR $d_f := \{(x,\sigma,i) : x \xmapsto{i \text{ STEPS}} \sigma\}$
  - Π "UNAMBIGUOUS" [RRR16]
  - $x \longmapsto f(x)$ "STRUCTURED"

"CRYPTO PART"

- DESIGN HASH FUNCTION H SUCH THAT $\widetilde{\Pi}$ IS SOUND

$\Pi \xrightarrow{H} \widetilde{\Pi}$

THE TOOLBOX

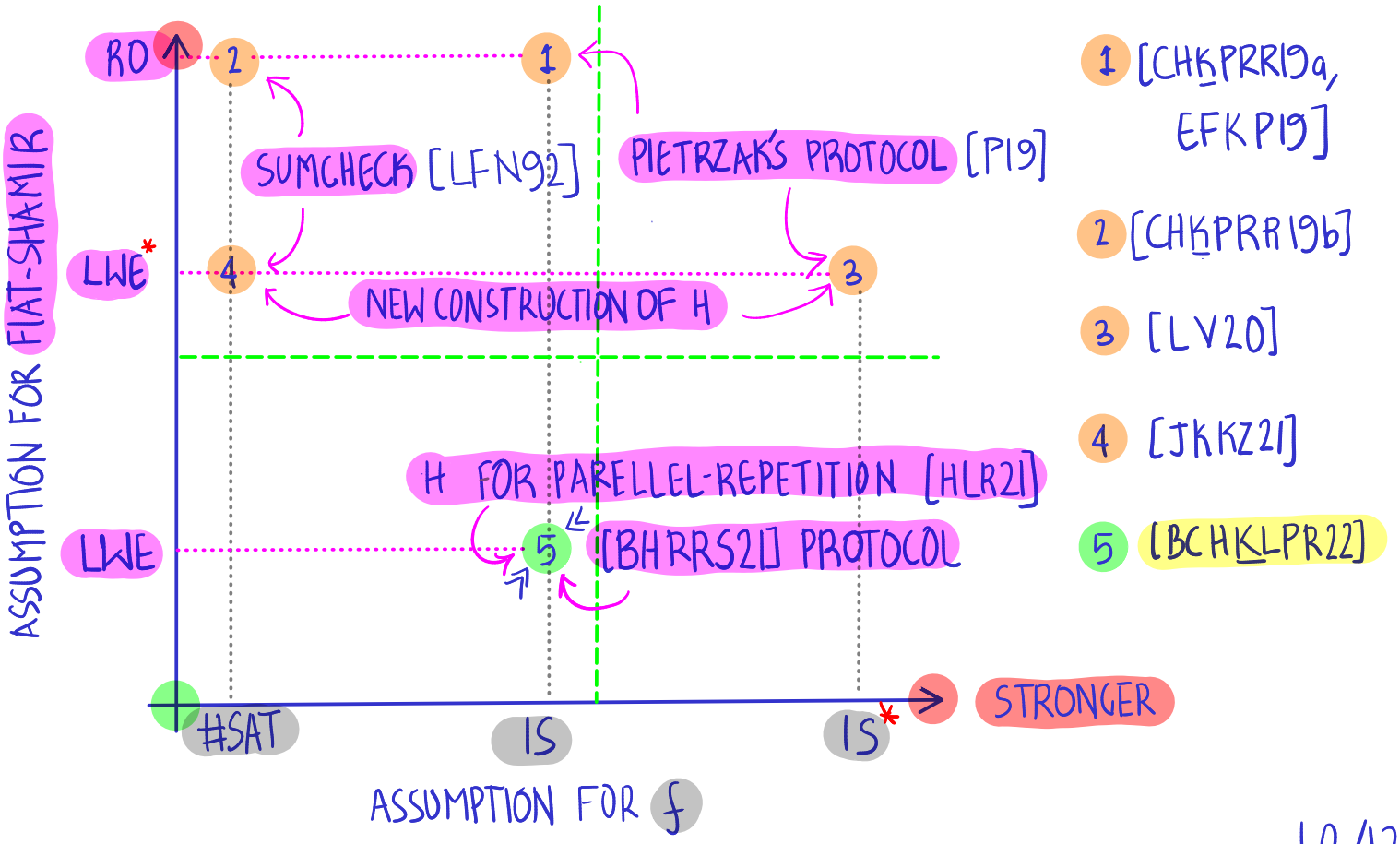
HARD-TO-COMPUTE fs:

- #SAT $f(C) :=$ #ASSIGNMENTS SATISFYING C (C: CNF)
- ITERATED SQUARING (IS) $\leqslant$ FACTORING
  $f(g,T) := g^{2^T}$ OVER $\mathbb{G}$ ($g \in \mathbb{G}$)
  GROUP OF UNKNOWN ORDER (EG: RSA GROUP)
- IS* ← STRONG VARIANTS

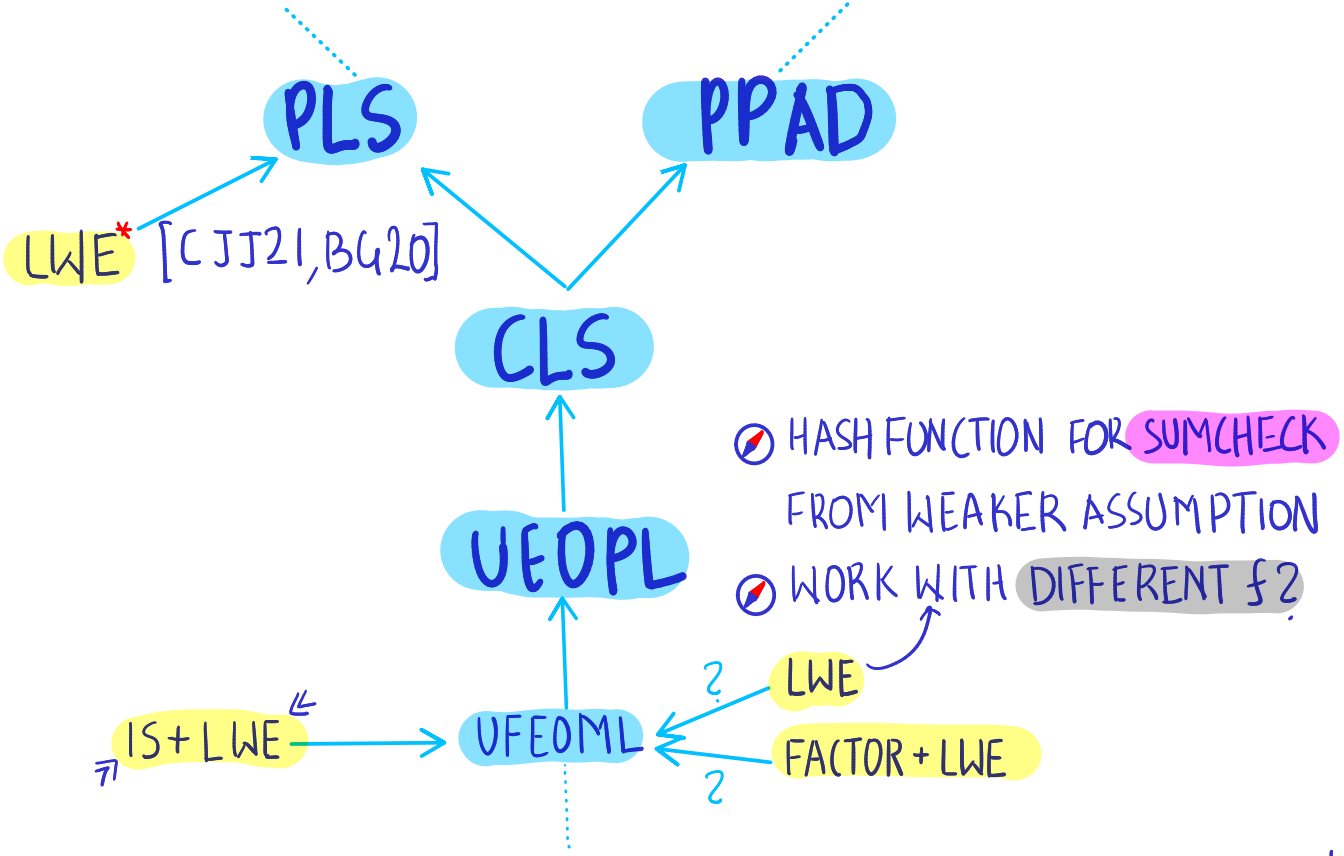
ASSUMPTIONS TO CONSTRUCT H

- RANDOM ORACLE (RO)
- LEARNING WITH ERRORS (LWE)
  "SOLVE SYSTEM OF NOISY LINEAR EQUATIONS"
- LWE* → STRONG VARIANTS

RECENT ADVANCES



OPEN QUESTIONS




THANK YOU!
FNDP
HAS
FITISHAMIR
ASSUMPTIO
SNIOFIDAG
PROOF
SYSTEM
COLLISION
FEOML