

PPAD IS AS HARD AS LWE & ITERATED SQUARING

NIR BITANSKY



ARKARAI CHOUDHURI JUSTIN HOLMGREN



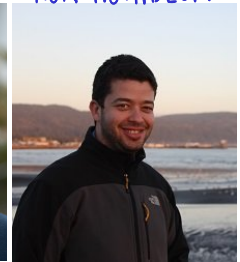
ALEX LOMBARDI



OMER PANETH



RON ROTHBLUM



CHEZHAN KAMATH

NTT RESEARCH

TEL AVIV UNIVERSITY

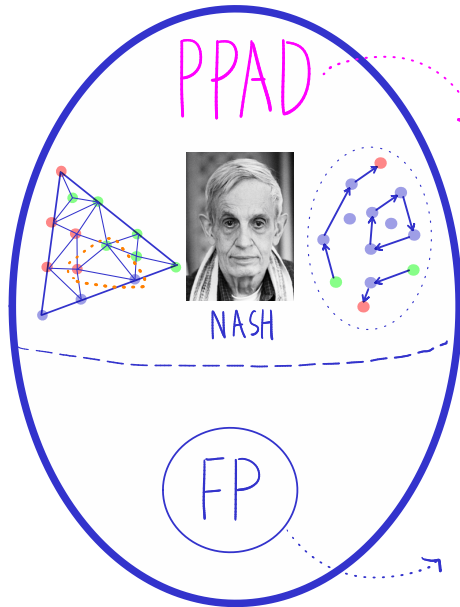
TECHNION

BERKELEY

SIMONS INSTITUTE

TCC 2022, NOV. 6-10, CHICAGO

PPAD

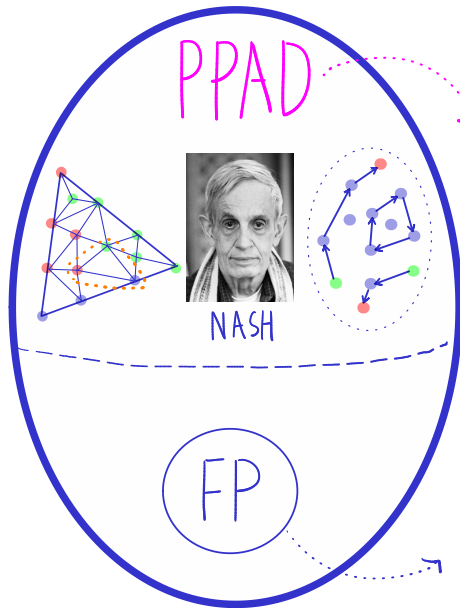


POLI. PARITY ARGUMENT ON DIGRAPHS

◆ CLASS OF SEARCH PROBLEMS

→ EASY SEARCH PROBLEMS

PPAD



POLY. PARITY ARGUMENT ON DIGRAPHS

◆ CLASS OF SEARCH PROBLEMS

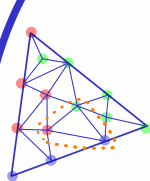
EASY SEARCH PROBLEMS

⇒ CRYPTO $\overset{?}{\rightarrow}$ PPAD IS HARD \nwarrow

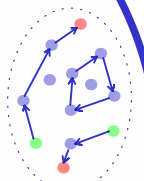
PPAD \subseteq TFNP

TOTAL FUNCTIONAL NP

PPAD



NASH



POLY. PARITY ARGUMENT ON DIGRAPHS

◆ CLASS OF SEARCH PROBLEMS

FP

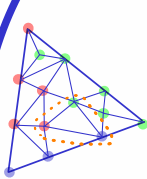
→ EASY SEARCH PROBLEMS

⇒ CRYPTO $\overset{?}{\rightarrow}$ PPAD IS HARD \leftarrow

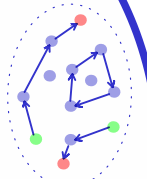
PPAD \subseteq TFNP

TOTAL FUNCTIONAL NP

PPAD



NASH



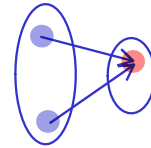
POLY. PARITY ARGUMENT ON DIGRAPHS

◆ CLASS OF SEARCH PROBLEMS

● FACTOR

● COLLISION

$2041 = 20 \times 41$



FP

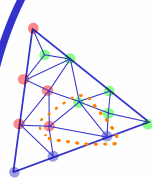
EASY SEARCH PROBLEMS

\Rightarrow CRYPTO $\stackrel{?}{\rightarrow}$ PPAD IS HARD \Leftarrow

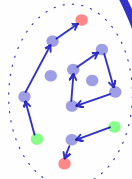
PPAD \subseteq TFNP

TOTAL FUNCTIONAL NP

PPAD



NASH



POLY. PARITY ARGUMENT ON DIGRAPHS

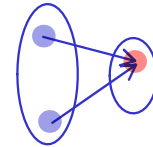
◆ CLASS OF SEARCH PROBLEMS

?

● FACTOR

● COLLISION

$2041 = 20 \times 41$

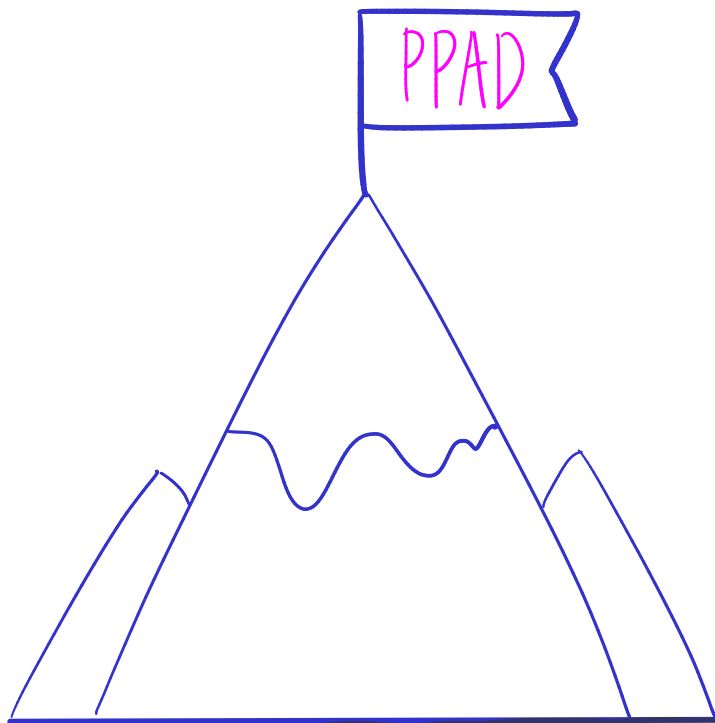


FP

EASY SEARCH PROBLEMS

\Rightarrow CRYPTO $\stackrel{?}{\rightarrow}$ PPAD IS HARD \Leftarrow

CRYPTO \Rightarrow PPAD IS HARD



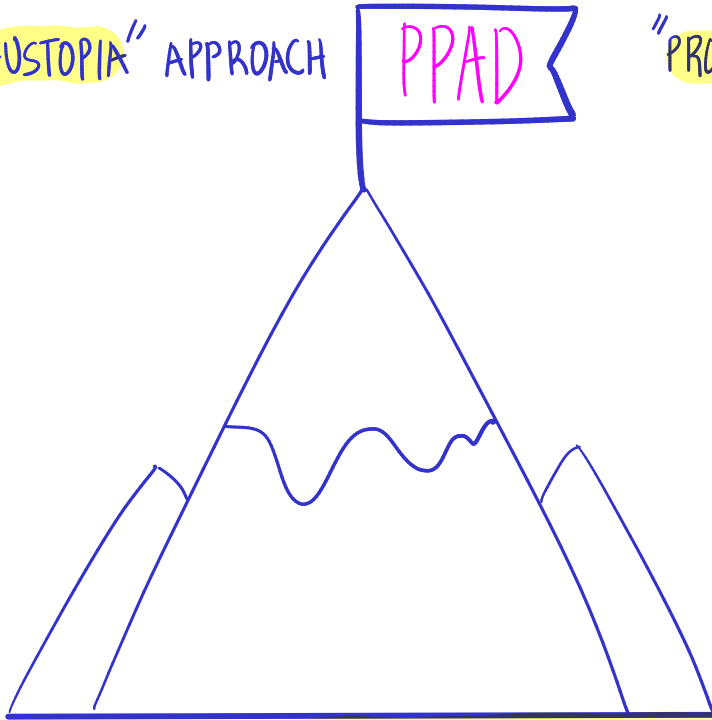
STANDARD CRYPTO : WELL-STUDIED, POLY. ASSUMPTIONS

CRYPTO \Rightarrow PPAD IS HARD

"OBFUSTOPIA" APPROACH

PPAD

"PROOF SYSTEM" APPROACH



STANDARD CRYPTO : WELL-STUDIED, POLY. ASSUMPTIONS

CRYPTO \Rightarrow PPAD IS HARD

"OBFUSTOPIA" APPROACH

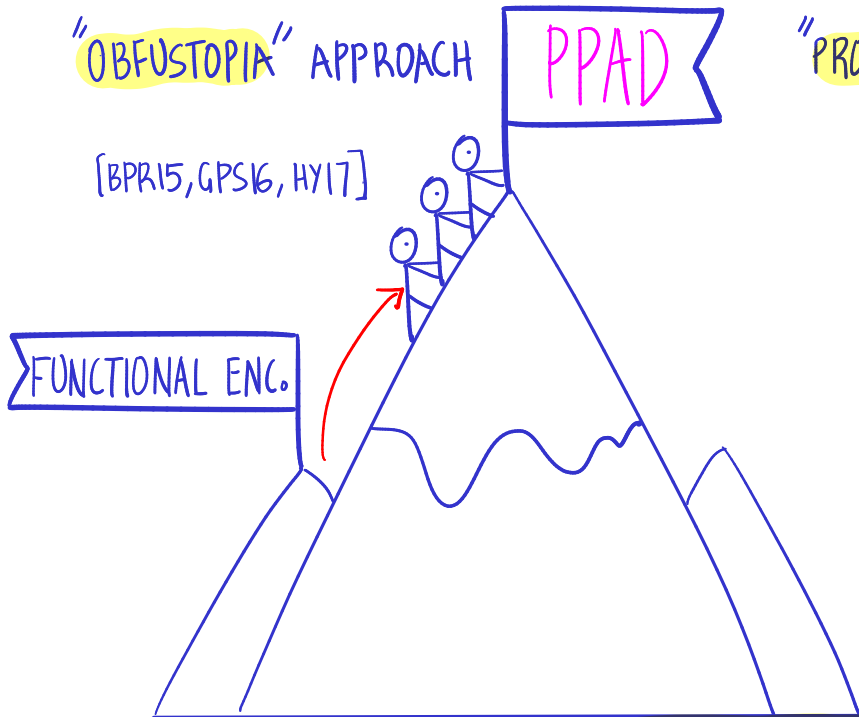
[BPR15, GPS16, HY17]

PPAD

"PROOF SYSTEM" APPROACH

FUNCTIONAL ENC.

STANDARD CRYPTO : WELL-STUDIED, POLY. ASSUMPTIONS



CRYPTO \Rightarrow PPAD IS HARD

"OBFUSTOPIA" APPROACH

[BPR15, GPS16, HY17]

PPAD

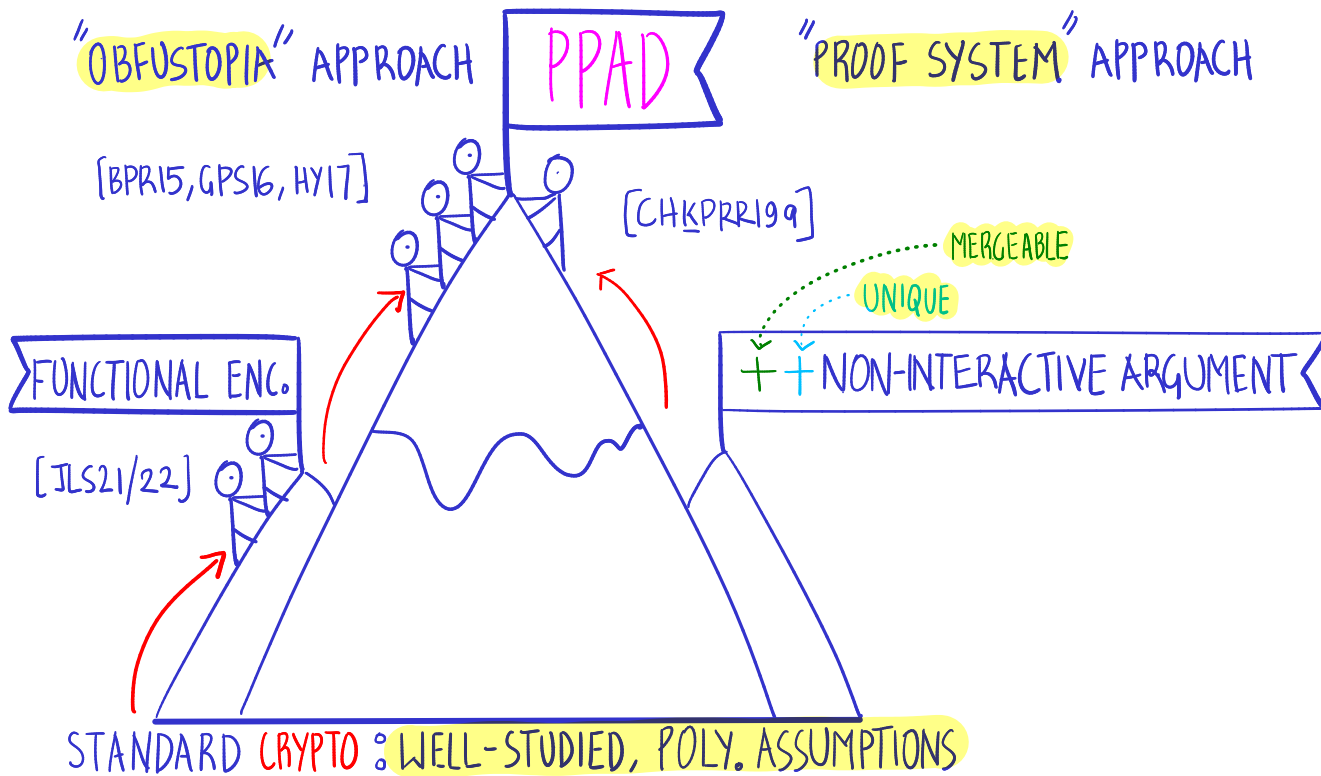
"PROOF SYSTEM" APPROACH

FUNCTIONAL ENC.

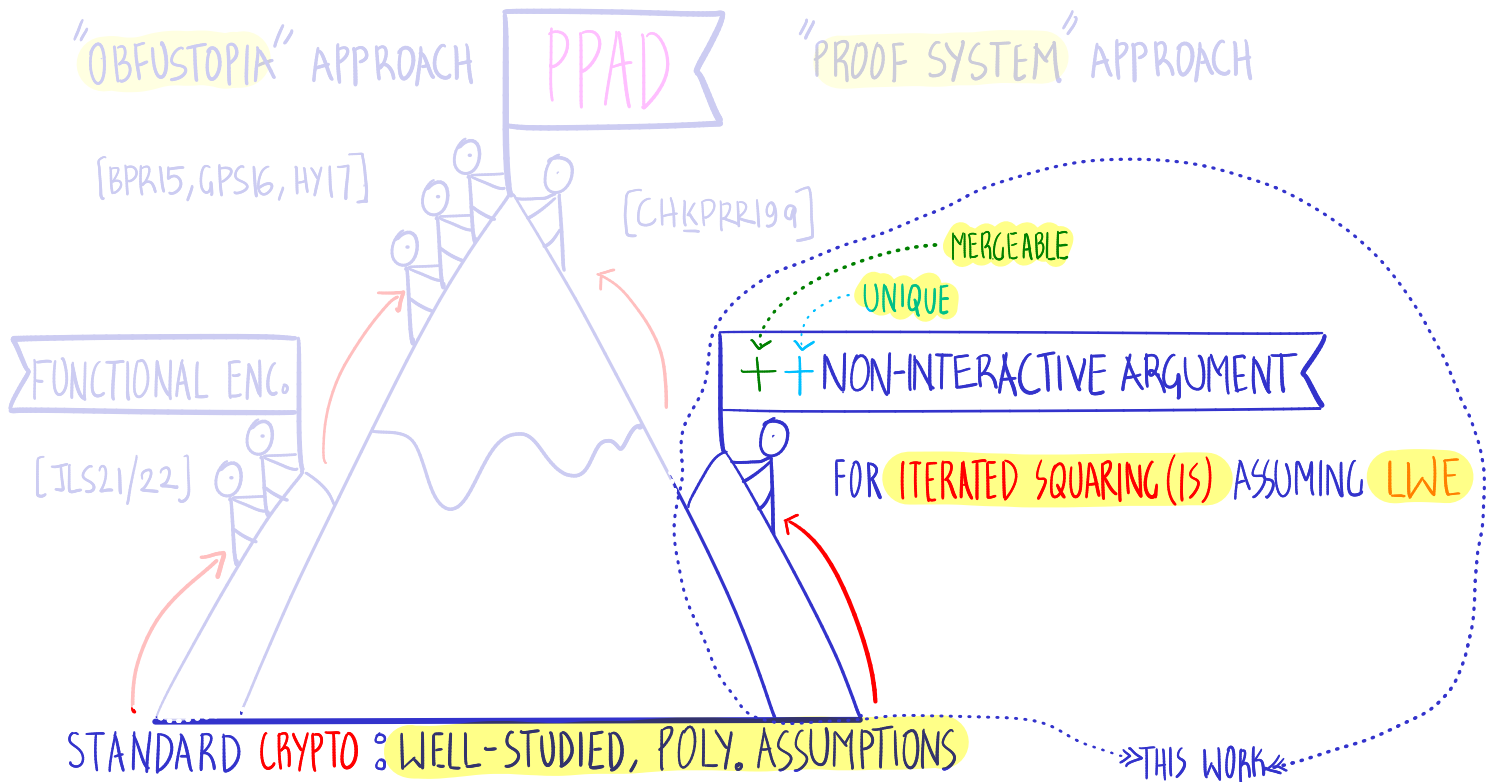
[JLS21/22]

STANDARD CRYPTO : WELL-STUDIED, POLY. ASSUMPTIONS

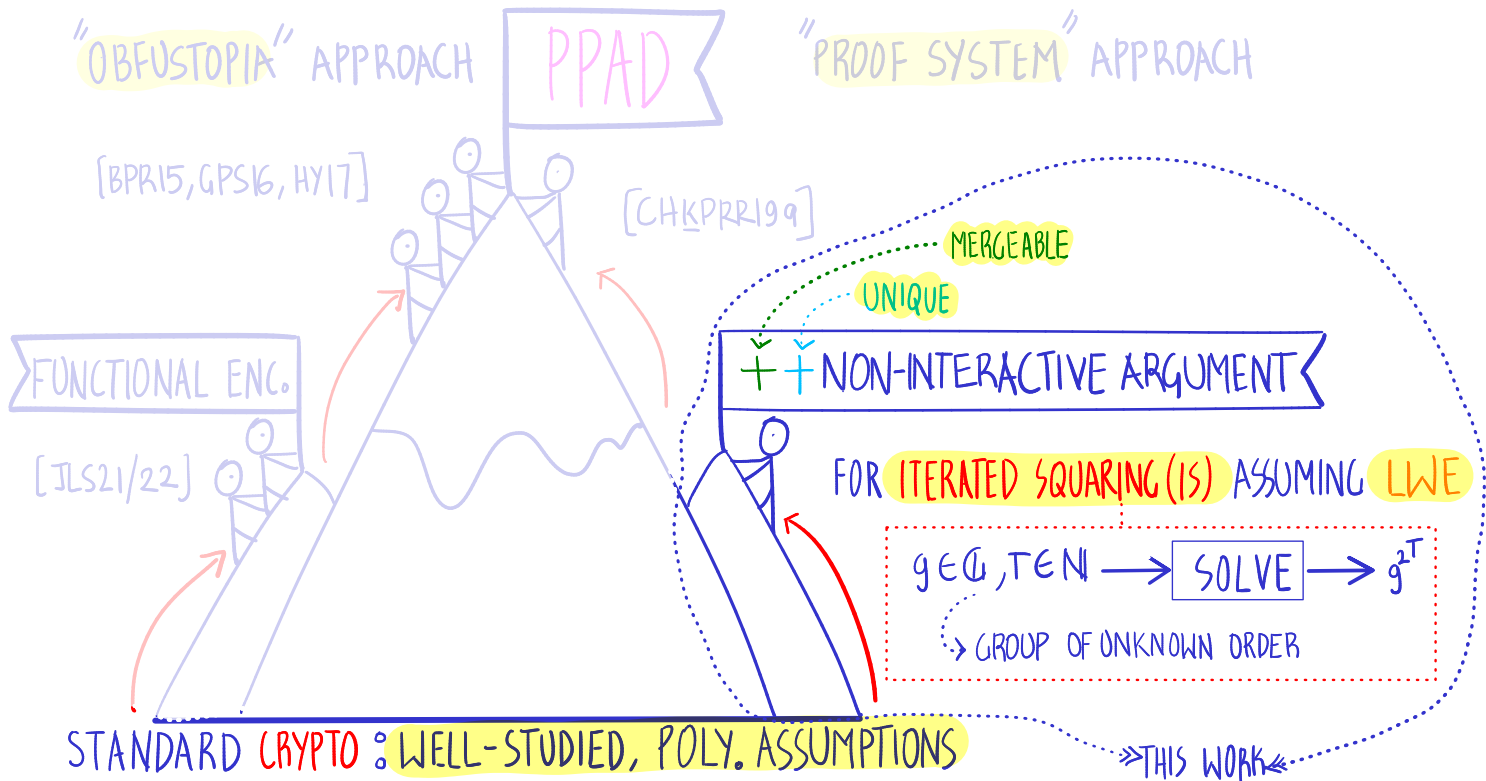
CRYPTO \Rightarrow PPAD IS HARD



CRYPTO \Rightarrow PPAD IS HARD

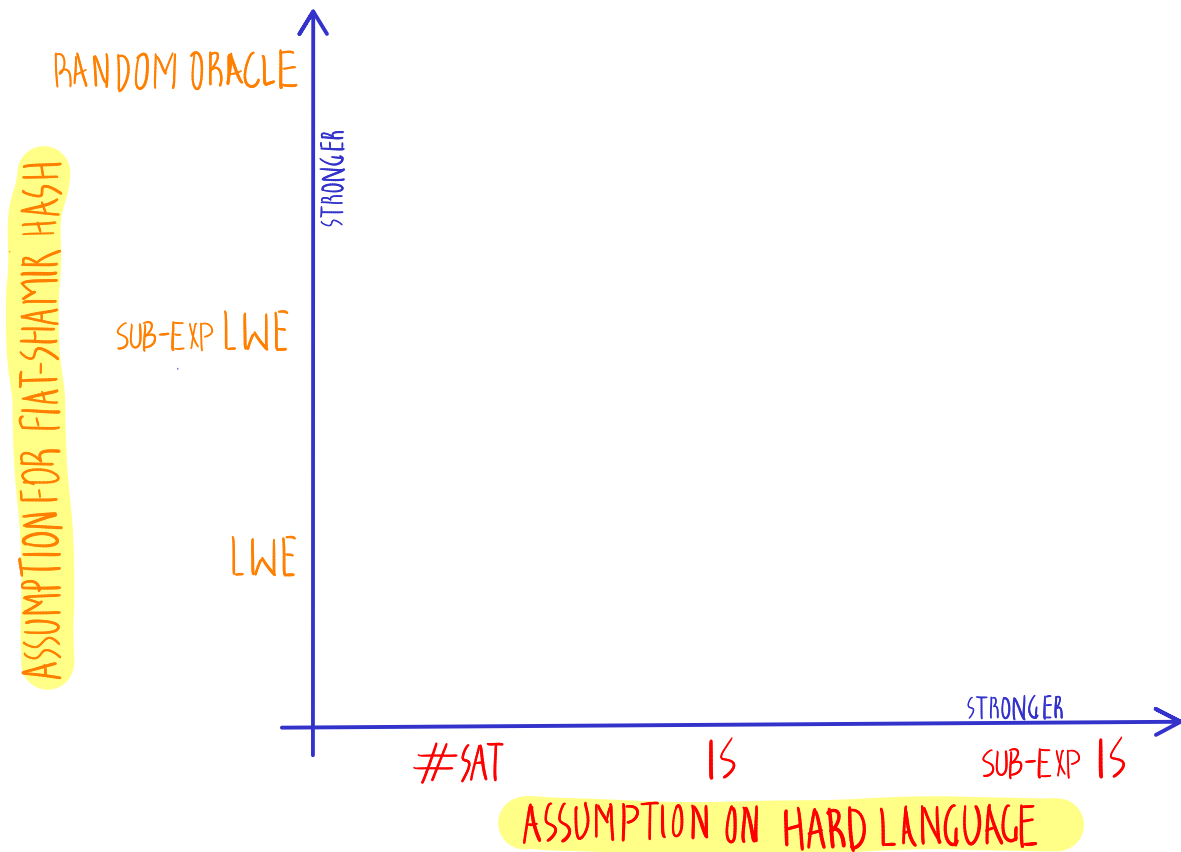


CRYPTO \Rightarrow PPAD IS HARD

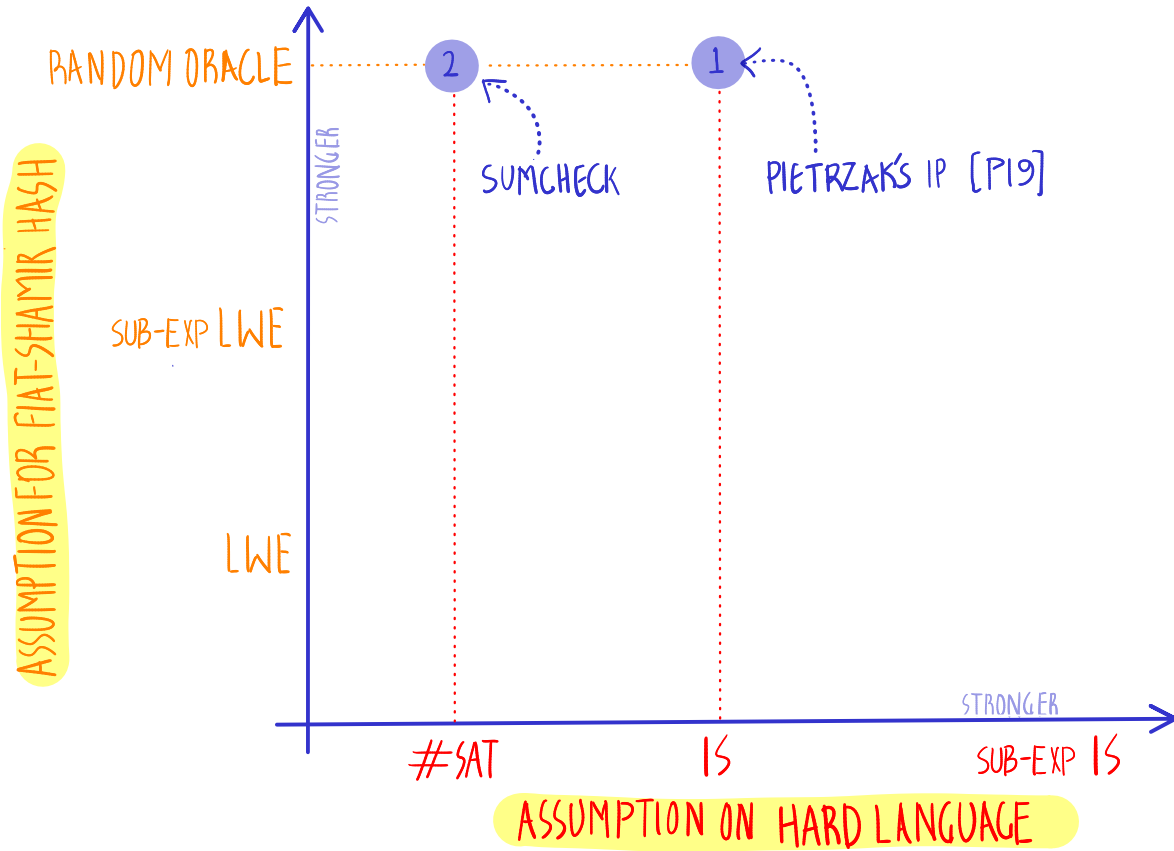


++IP FOR \mathcal{L} FIAT-SHAMIR \Rightarrow ++NI-ARG FOR \mathcal{L}

++IP FOR \mathcal{L} FIAT-SHAMIR \implies ++NI-ARG FOR \mathcal{L}

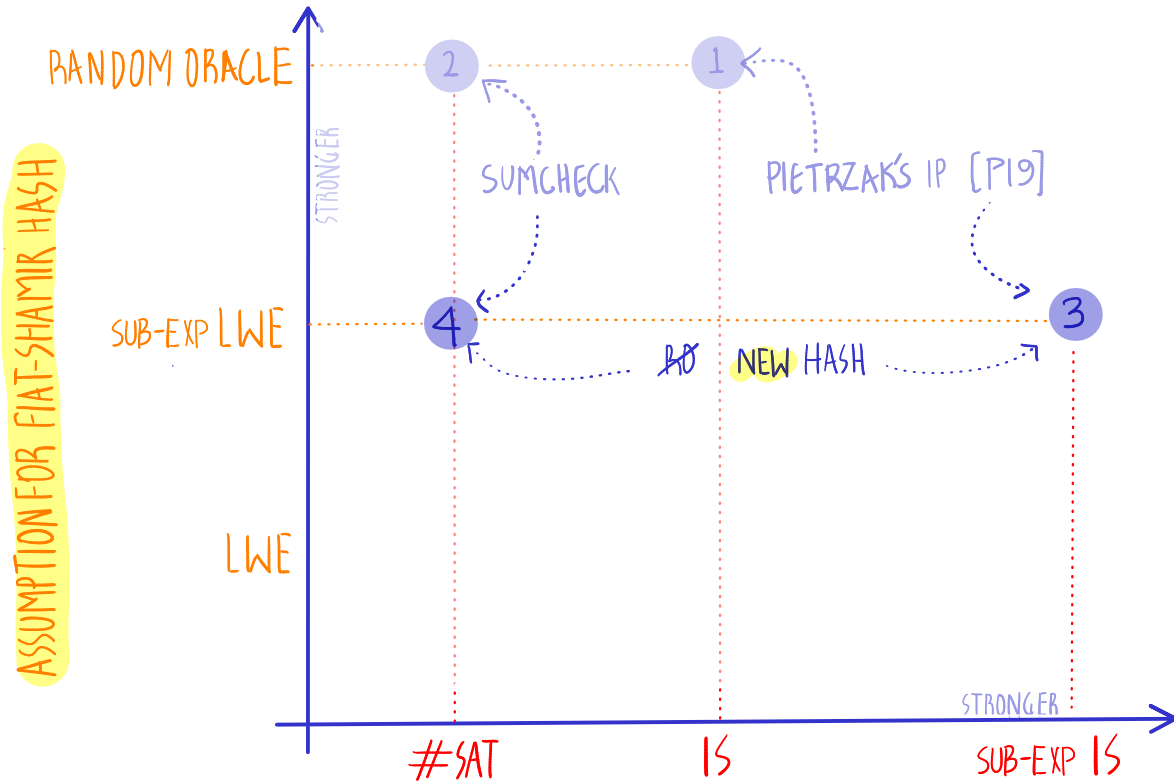


++IP FOR \mathcal{L} FIAT-SHAMIR \implies ++NI-ARG FOR \mathcal{L}



1 [CHKPRR19a, EFK P19] 2 [CHKPRR19b]

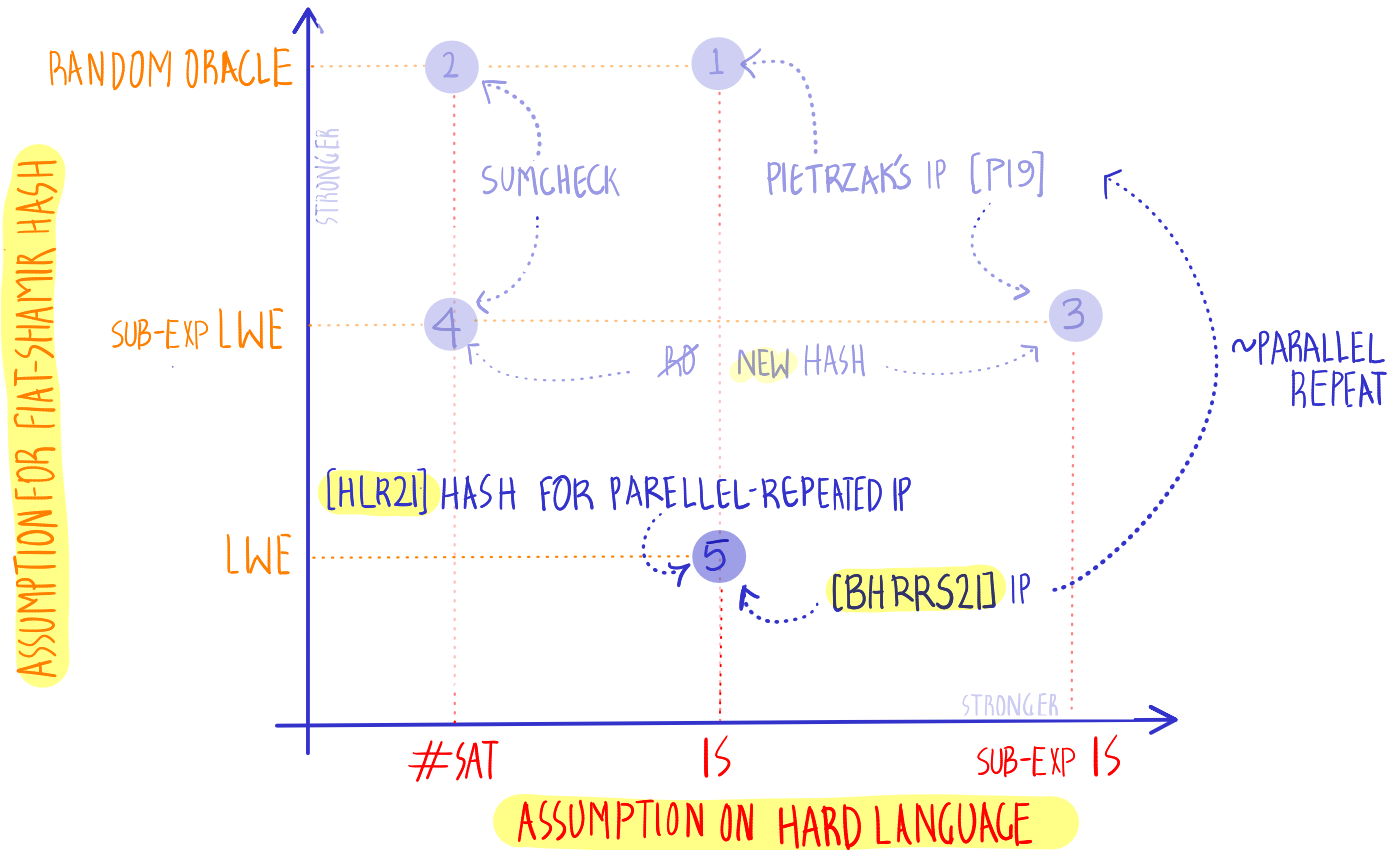
++IP FOR \mathcal{L} FIAT-SHAMIR \implies ++NI-ARG FOR \mathcal{L}



ASSUMPTION ON HARD LANGUAGE

- 1 [CHK_PRR19a, EFK_P19]
- 2 [CHK_PRR19b]
- 3 [LV20]
- 4 [JKKZ21]

++IP FOR \mathcal{L} FIAT-SHAMIR \implies ++NI-ARG FOR \mathcal{L}

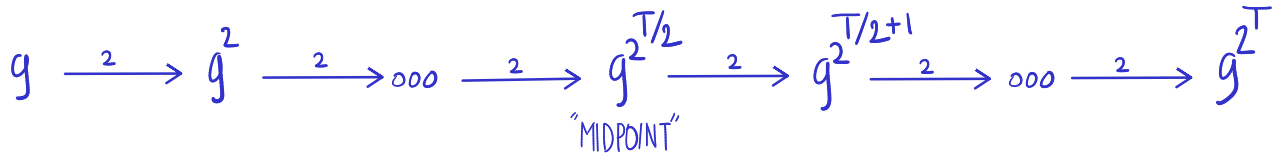
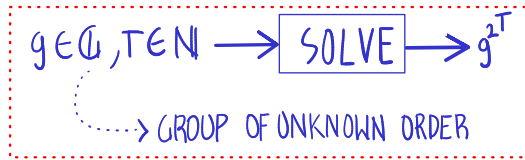


- 1 [CHK_PRR19a, EFK_P19] 2 [CHK_PRR19b] 3 [LV20] 4 [JKK21] 5 [THIS WORK]

++NI-ARG

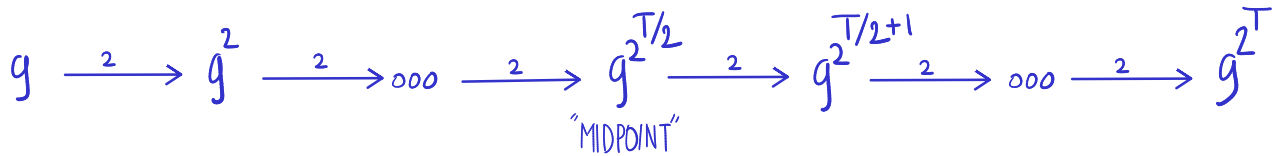
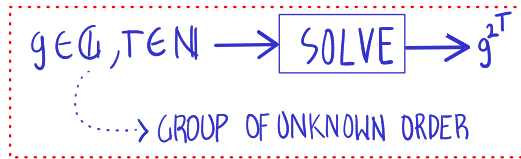
++ NI-ARG FOR $\alpha_{IS} \triangleq \{(g, T, h) : g^{2^T} = h\}$

ITERATED SQUARING (IS)



++ NI-ARG FOR $\alpha_{IS} \triangleq \{(g, T, h) : g^{2^T} = h\}$

ITERATED SQUARING (IS)



+ MERGEABLE

PROOFS OF SMALL RELATED STATEMENTS

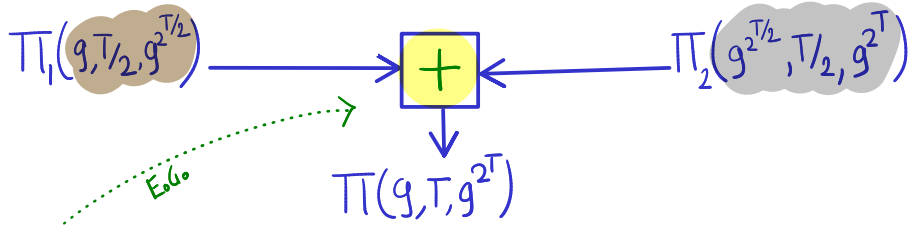
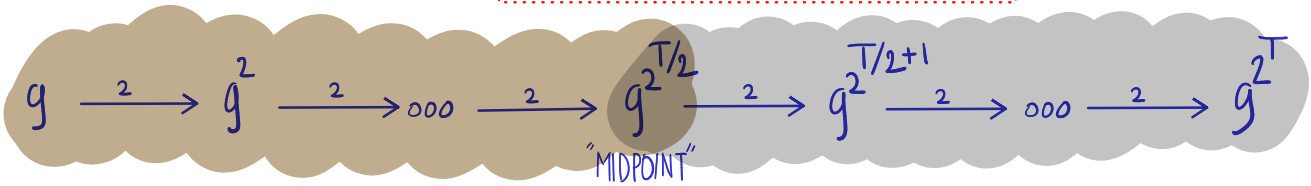
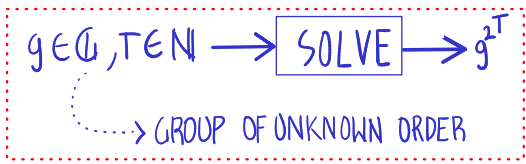


PROOF OF LARGER STATEMENT

FASTER THAN COMPUTING FROM SCRATCH

++ NI-ARG FOR $\mathcal{L}_{IS} \triangleq \{(g, T, h) : g^{2^T} = h\}$

ITERATED SQUARING (IS)



+ MERGEABLE

PROOFS OF SMALL RELATED STATEMENTS

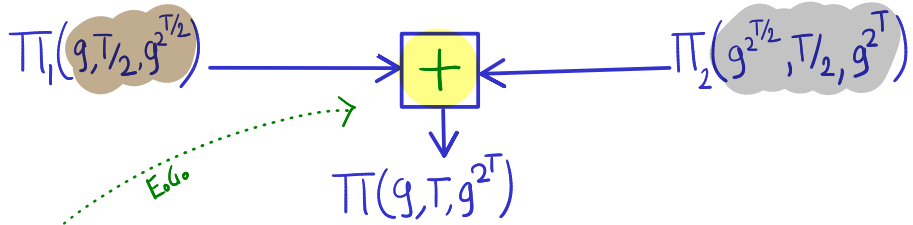
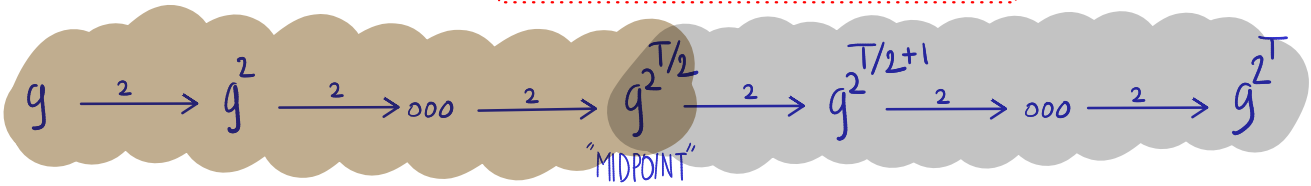
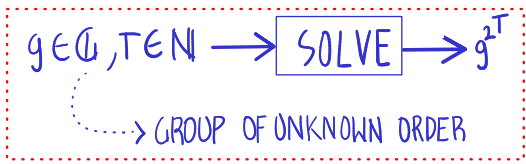


PROOF OF LARGER STATEMENT

FASTER THAN COMPUTING FROM SCRATCH

++ NI-ARG FOR $\mathcal{L}_{IS} \triangleq \{(g, T, h) : g^{2^T} = h\}$

ITERATED SQUARING (IS)



+ MERGEABLE

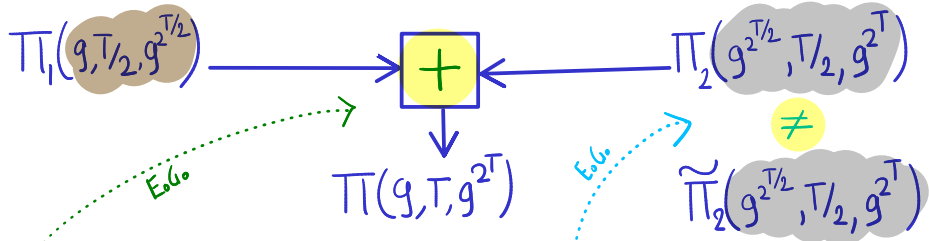
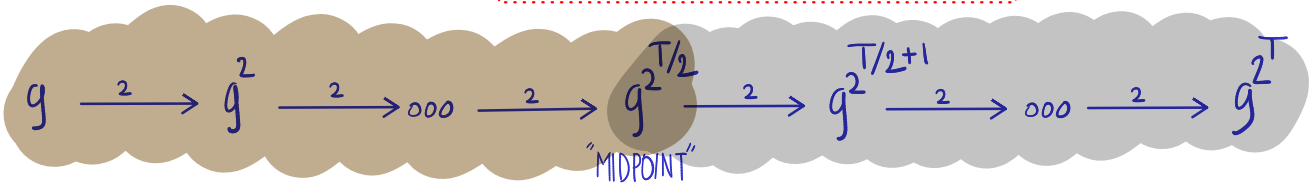
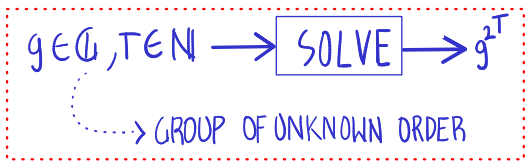
PROOFS OF SMALL RELATED STATEMENTS
 ↓
 PROOF OF LARGER STATEMENT
 FASTER THAN COMPUTING FROM SCRATCH

+ UNIQUE

HARD TO FIND TWO PROOFS FOR
 A TRUE STATEMENT

++ NI-ARG FOR $\mathcal{L}_{IS} \triangleq \{(g, T, h) : g^{2^T} = h\}$

ITERATED SQUARING (IS)



+ MERGEABLE

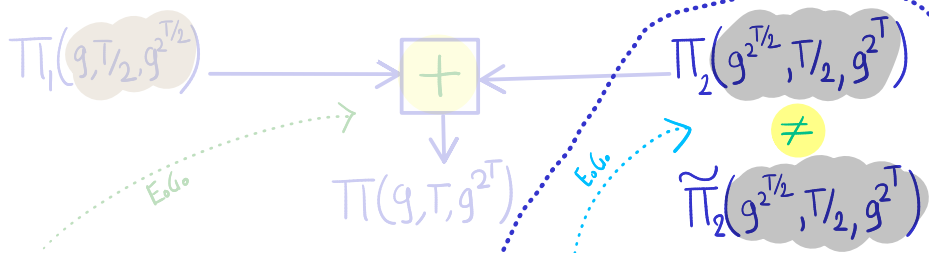
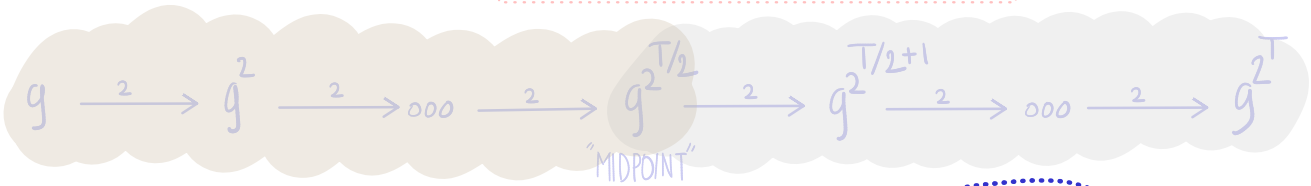
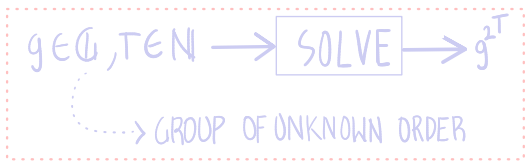
PROOFS OF SMALL RELATED STATEMENTS
 ↓
 PROOF OF LARGER STATEMENT
 FASTER THAN COMPUTING FROM SCRATCH

+ UNIQUE

HARD TO FIND TWO PROOFS FOR
 A TRUE STATEMENT

++ NI-ARG FOR $\mathcal{L}_{IS} \triangleq \{(g, T, h) : g^{2^T} = h\}$

ITERATED SQUARING (IS)



+ MERGEABLE

PROOFS OF SMALL RELATED STATEMENTS
 ↓
 PROOF OF LARGER STATEMENT
 FASTER THAN COMPUTING FROM SCRATCH

+ UNIQUE

HARD TO FIND TWO PROOFS FOR
 A TRUE STATEMENT

» FOCUS «

++ NI-ARG FOR $\mathcal{L}_{1s} \triangleq \{(g, \tau, h) : g^{\tau} = h\}$

ATTEMPT 1: PIETRZAK'S IP [PI9]

+ UNIQUE ?

SOUND ?

FIAT-SHAMIR ?

++ NI-ARG FOR $\mathcal{L}_{1s} \triangleq \{(g, T, h) : g^{2^T} = h\}$

ATTEMPT 1: PIETRZAK'S IP [PI9]

(g, T, h)

\mathcal{P}

\mathcal{V}

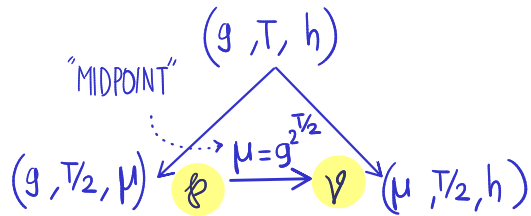
+ UNIQUE?

SOUND?

FIAT-SHAMIR?

++ NI-ARG FOR $\mathcal{L}_{1s} \triangleq \{(g, T, h) : g^{2^T} = h\}$

ATTEMPT 1: PIETRZAK'S IP [PI9]



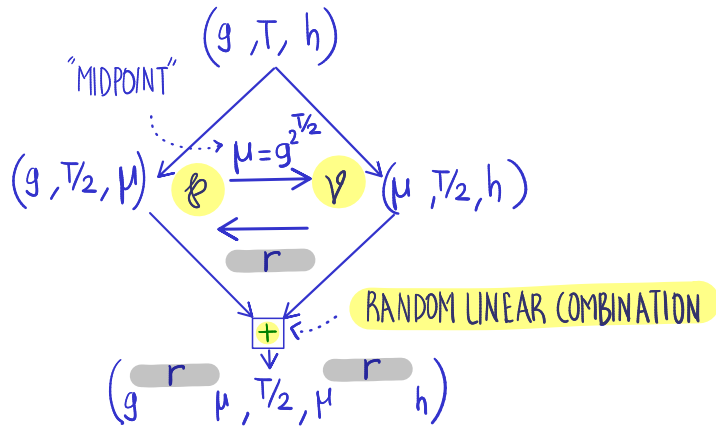
+ UNIQUE ?

SOUND ?

FIAT-SHAMIR ?

++ NI-ARG FOR $\mathcal{L}_{1s} \triangleq \{(g, T, h) : g^{2^T} = h\}$

ATTEMPT 1: PIETRZAK'S IP [PI9]



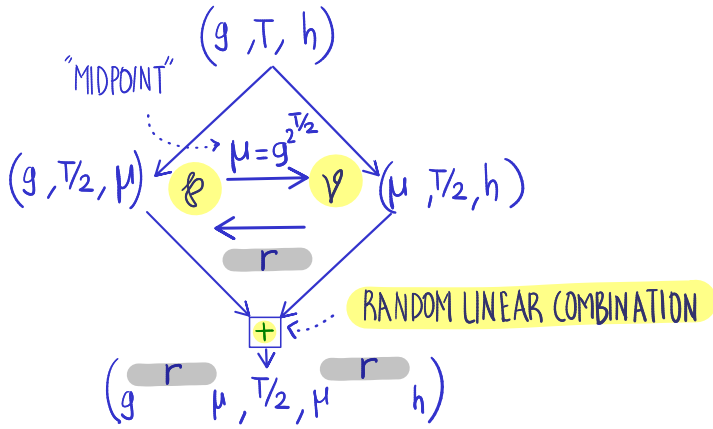
+ UNIQUE?

SOUND?

FIAT-SHAMIR?

++ NI-ARG FOR $\mathcal{L}_{IS} \triangleq \{(g, T, h) : g^{2^T} = h\}$

ATTEMPT 1: PIETRZAK'S IP [PI9]



RECURSE $\dots \rightarrow \begin{matrix} \circ \\ \circ \\ \circ \end{matrix}$

$(g', 2, h')$ \leftarrow μ ACCEPTS IF $h' = (g')^2$

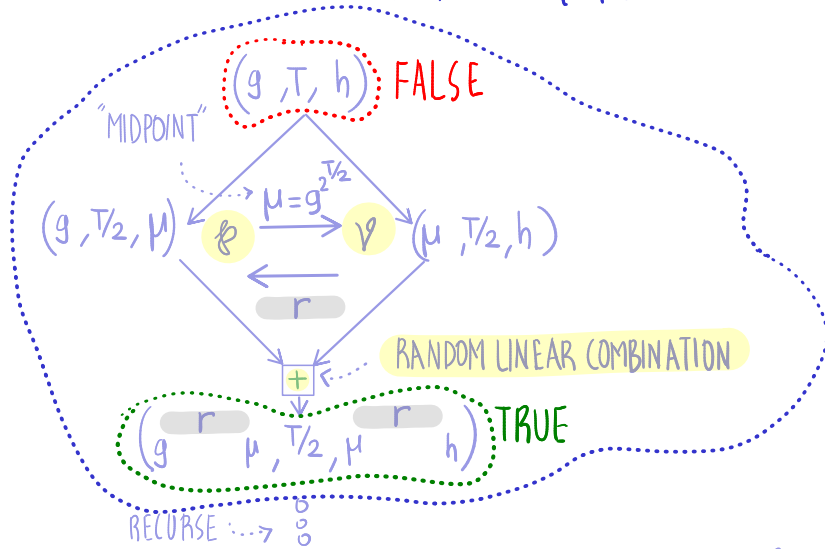
+ UNIQUE?

SOUND?

FIAT-SHAMIR?

++ NI-ARG FOR $\mathcal{L}_{IS} \triangleq \{(g, T, h) : g^{2^T} = h\}$

ATTEMPT 1: PIETRZAK'S IP [PI9]



$(g', 2, h') \leftarrow V$ ACCEPTS IF $h' = (g')^2$

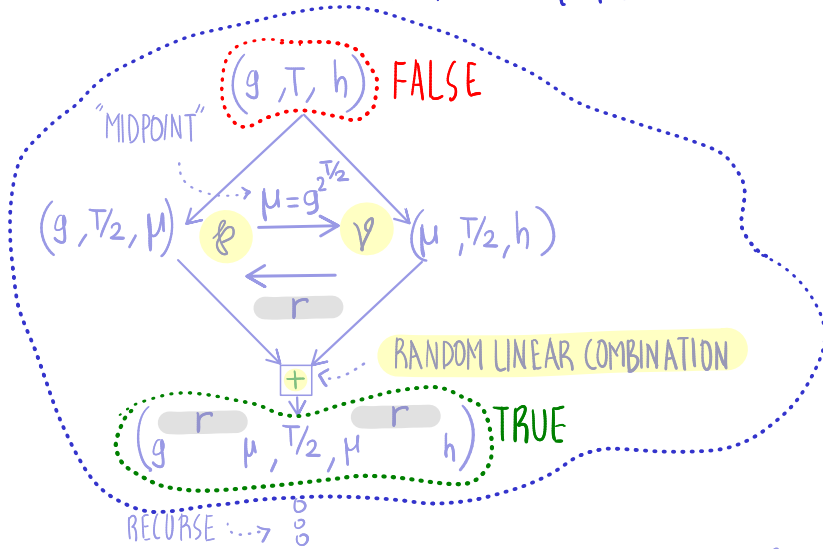
+ UNIQUE?

SOUND? \exists BAD $r \Rightarrow$ STATISTICAL SOUNDNESS

FIAT-SHAMIR?

++ NI-ARG FOR $\Delta_{15} \triangleq \{(g, T, h) : g^{2^T} = h\}$

ATTEMPT 1: PIETRZAK'S IP [PI9]



$(g', 2, h)$ $\leftarrow \mathcal{V}$ ACCEPTS IF $h' = (g')^2$

+ UNIQUE?

SOUND?



$\exists!$ BAD r

\Rightarrow STATISTICAL SOUNDNESS

FIAT-SHAMIR?

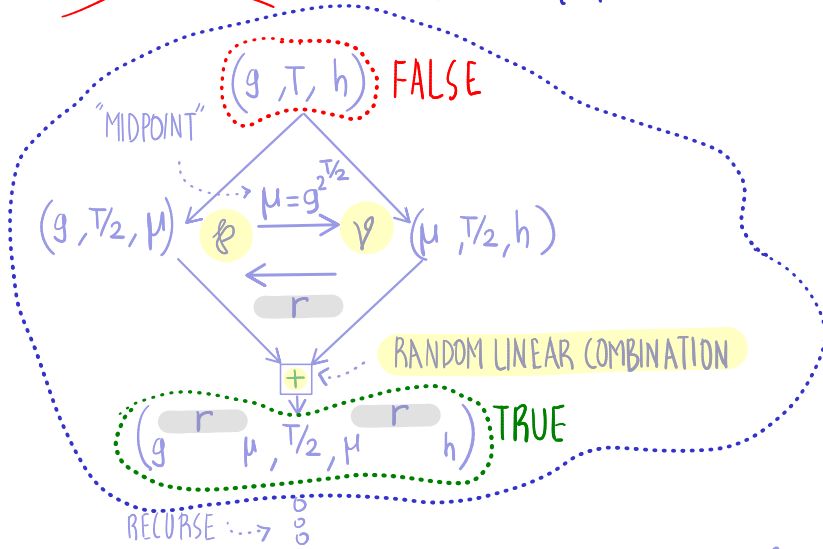


SOLVE DLP

\Rightarrow CANNOT USE [PSI9] HASH FROM LWE

++ NI-ARG FOR $\Delta_{15} \triangleq \{(g, T, h) : g^{2^T} = h\}$

~~ATTEMPT 1: PIETRZAK'S IP [PI9]~~



$(g', 2, h) \leftarrow \mathcal{V}$ ACCEPTS IF $h' = (g')^2$

+ UNIQUE?

SOUND?



$\exists!$ BAD r

\Rightarrow STATISTICAL SOUNDNESS

FIAT-SHAMIR?

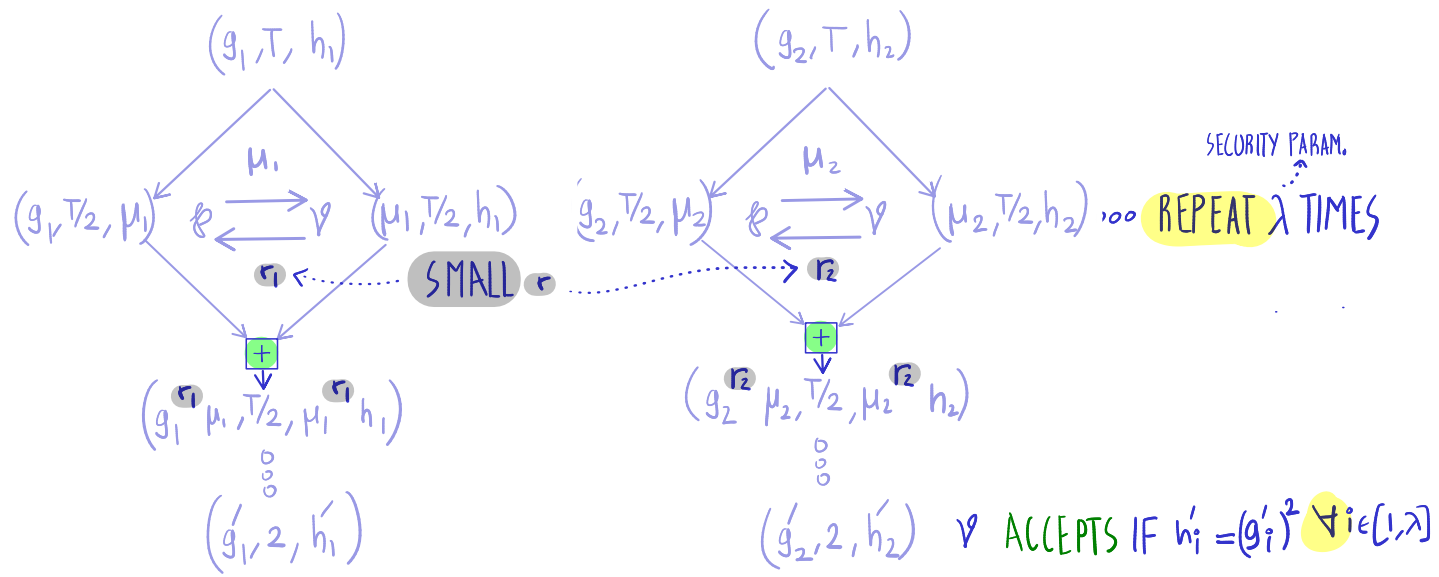


SOLVE DLP

\Rightarrow CANNOT USE [PSI9] HASH FROM LWE

++NI-ARG FOR $\mathcal{L}_{IS} \triangleq \{(g, T, h) : g^{2^T} = h\}$

ATTEMPT 2: PIETRZAK'S IP W/ "SMALL" r & PARALLEL REPETITION



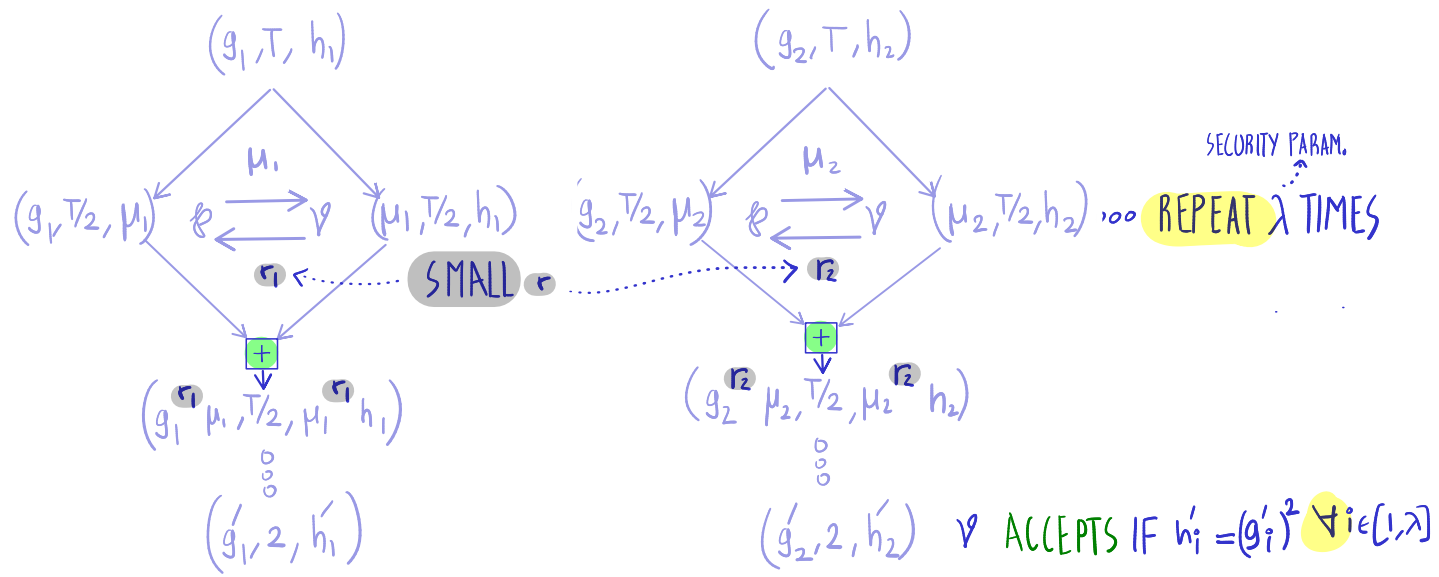
+UNIQUE ?

SOUND ?

FIAT-SHAMIR ?

++NI-ARG FOR $\mathcal{L}_{IS} \triangleq \{(g, T, h) : g^{2^T} = h\}$

ATTEMPT 2: PIETRZAK'S IP W/ "SMALL" r & PARALLEL REPETITION



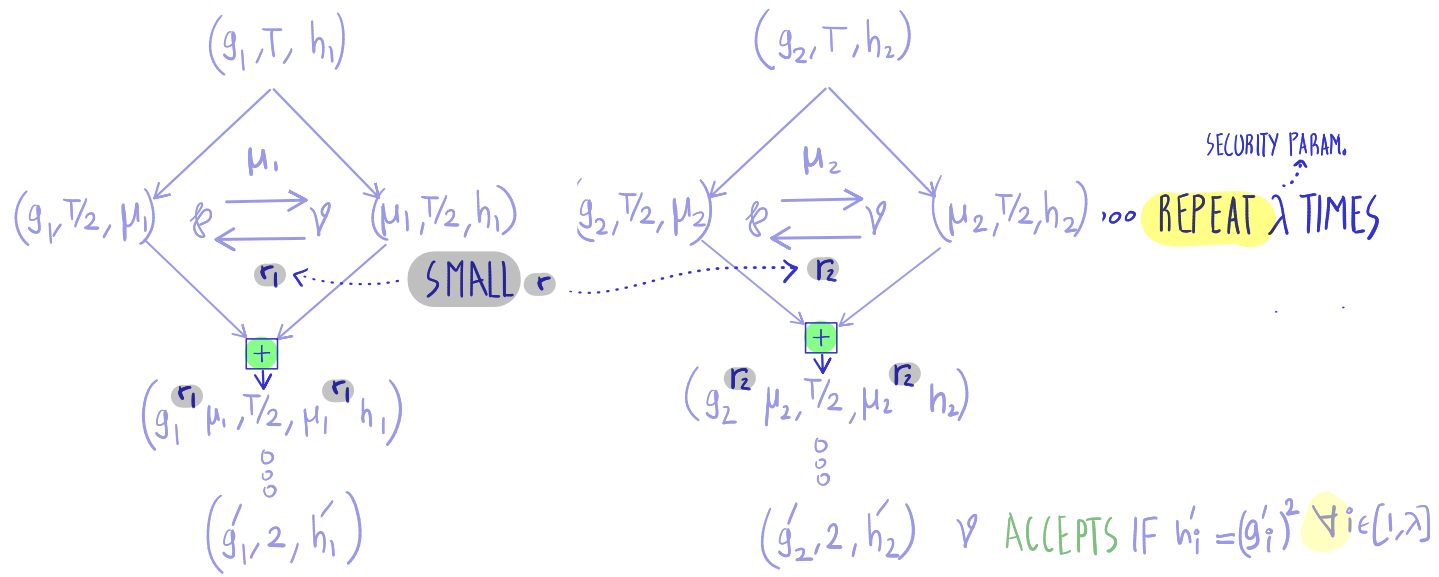
+UNIQUE?

SOUND? PARALLEL REP. AMPLIFIES SOUNDNESS

FIAT-SHAMIR? [HLR2] HASH FOR PARELLEL-REPEATED IP FROM LWE

++NI-ARG FOR $\mathcal{L}_{IS} \triangleq \{(g, T, h) : g^2 = h\}$

ATTEMPT 2: PIETRZAK'S IP W/ "SMALL" r & PARALLEL REPETITION



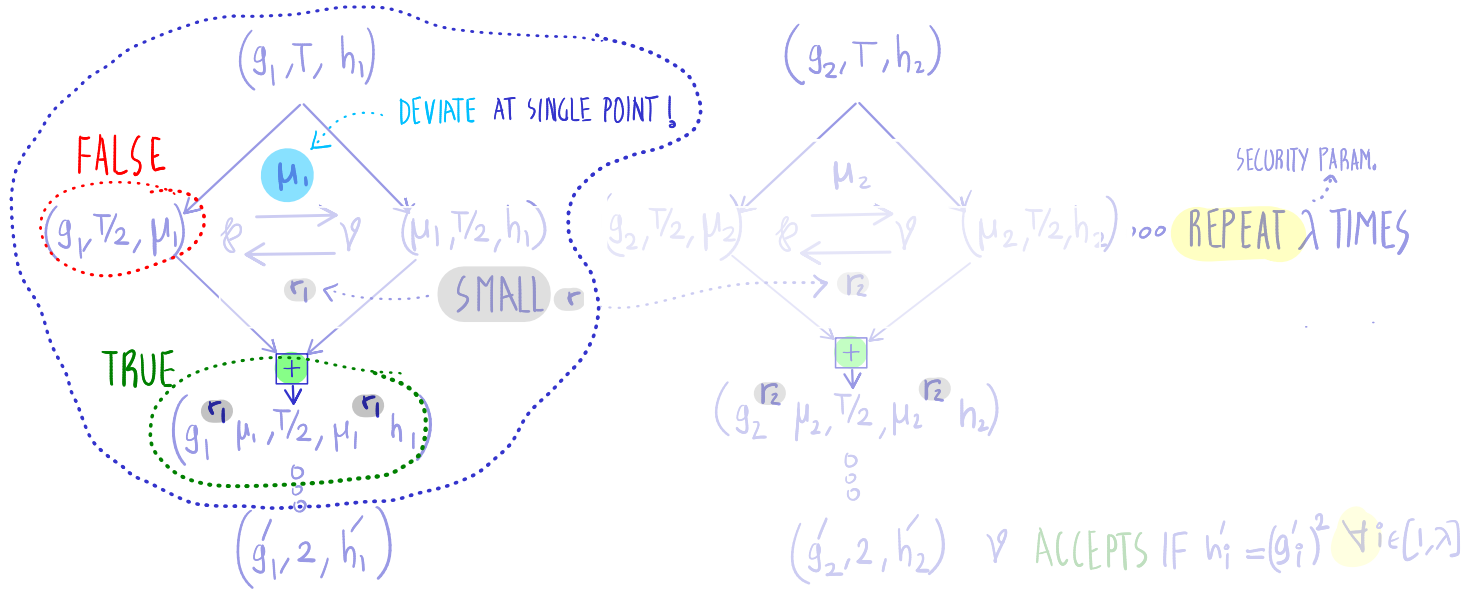
+UNIQUE? PARALLEL REP. DOESN'T PRESERVE UNIQUENESS! [RRR16]

SOUND? PARALLEL REP. AMPLIFIES SOUNDNESS

FIAT-SHAMIR? [HLR2] HASH FOR PARALLEL-REPEATED IP FROM LWE

++NI-ARG FOR $\mathcal{L}_{IS} \triangleq \{(g, T, h) : g^2 = h\}$

ATTEMPT 2: PIETRZAK'S IP W/ "SMALL" r & PARALLEL REPETITION



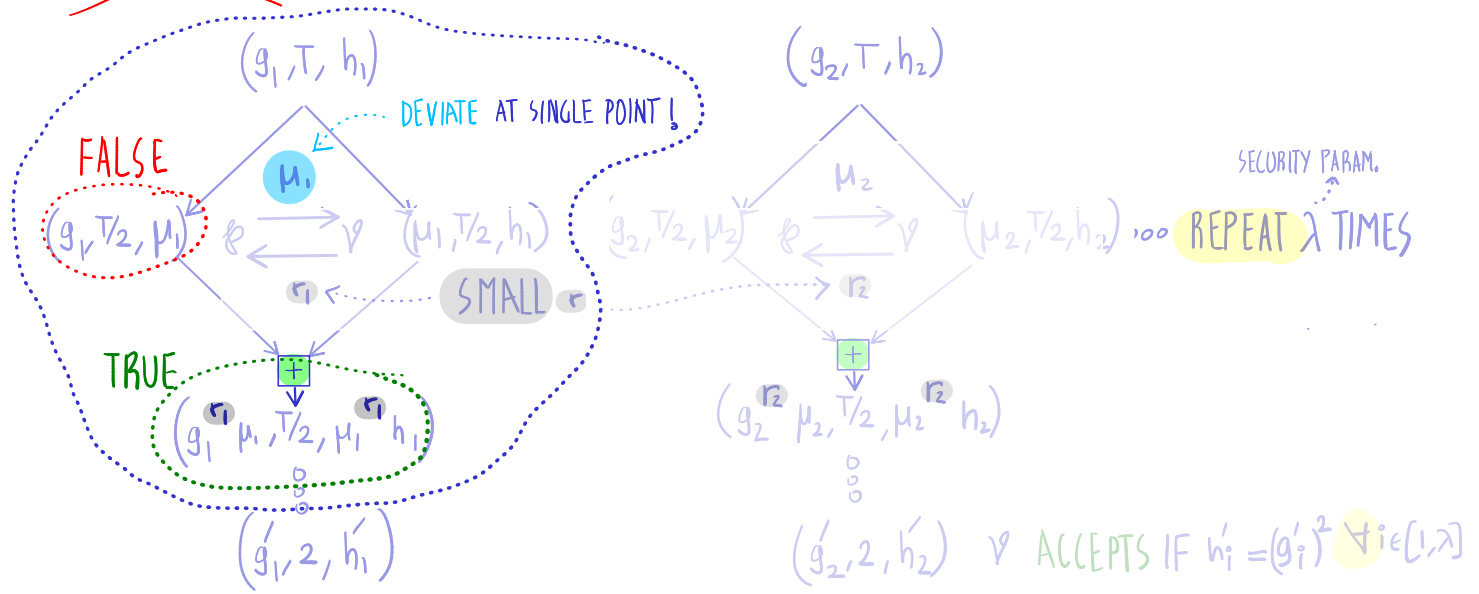
+UNIQUE? PARALLEL REP. DOESN'T PRESERVE UNIQUENESS! [RRR16]

SOUND? PARALLEL REP. AMPLIFIES SOUNDNESS

FIAT-SHAMIR? [HLR2] HASH FOR PARALLEL-REPEATED IP FROM LWE

++NI-ARG FOR $\mathcal{L}_{IS} \triangleq \{(g, T, h) : g^2 = h\}$

~~ATTEMPT 2: PIETRZAK'S IP W/ "SMALL" r & PARALLEL REPETITION~~



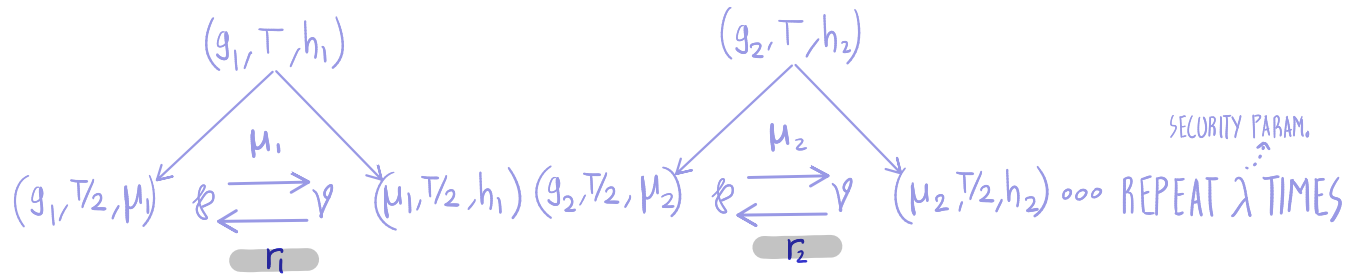
+UNIQUE? ✗ PARALLEL REP. DOESN'T PRESERVE UNIQUENESS! [RRR16]

SOUND? ✓ PARALLEL REP. AMPLIFIES SOUNDNESS

FIAT-SHAMIR? ✓ [HLR2] HASH FOR PARALLEL-REPEATED IP FROM LWE

++ NI-ARG FOR $\mathcal{L}_{1s} \triangleq \{(g, T, h) : g^2 = h\}$

OUR SOLUTION: MIX THE REPETITIONS! [BHARRS21]



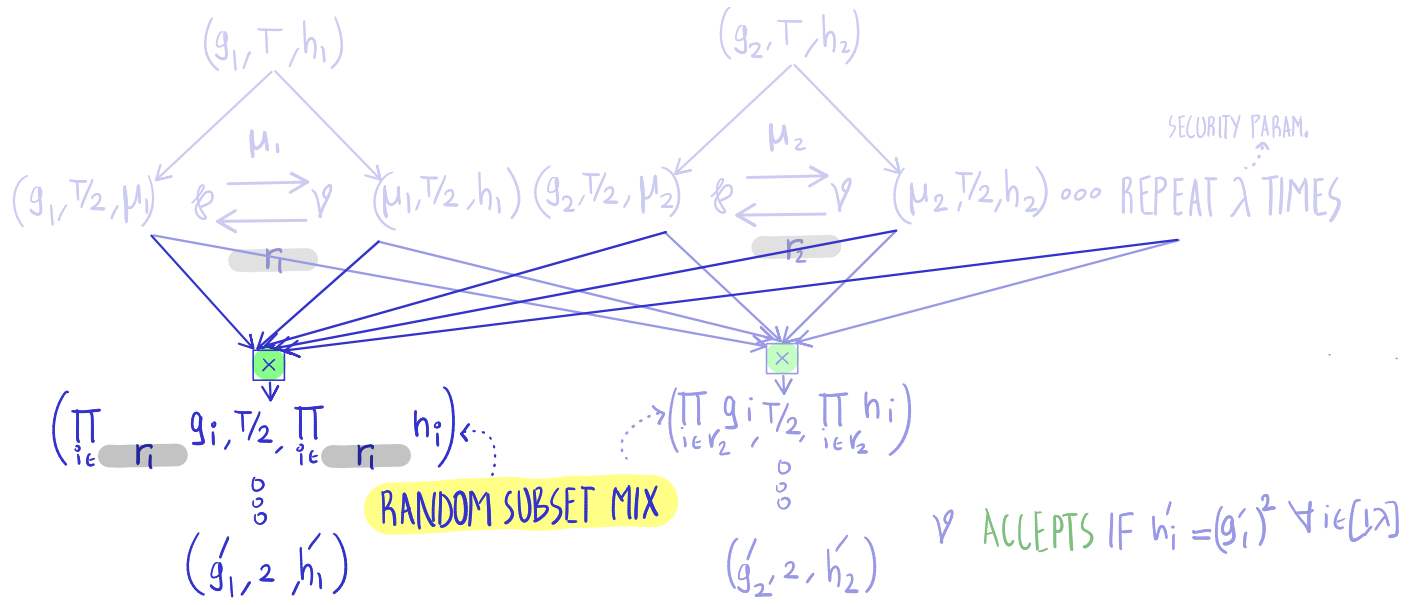
+ UNIQUE ?

SOUND ?

FIAT-SHAMIR ?

++ NI-ARG FOR $\mathcal{L}_{IS} \triangleq \{(g, T, h) : g^2 = h\}$

OUR SOLUTION: MIX THE REPETITIONS! [BHARRS21]



+ UNIQUE ?

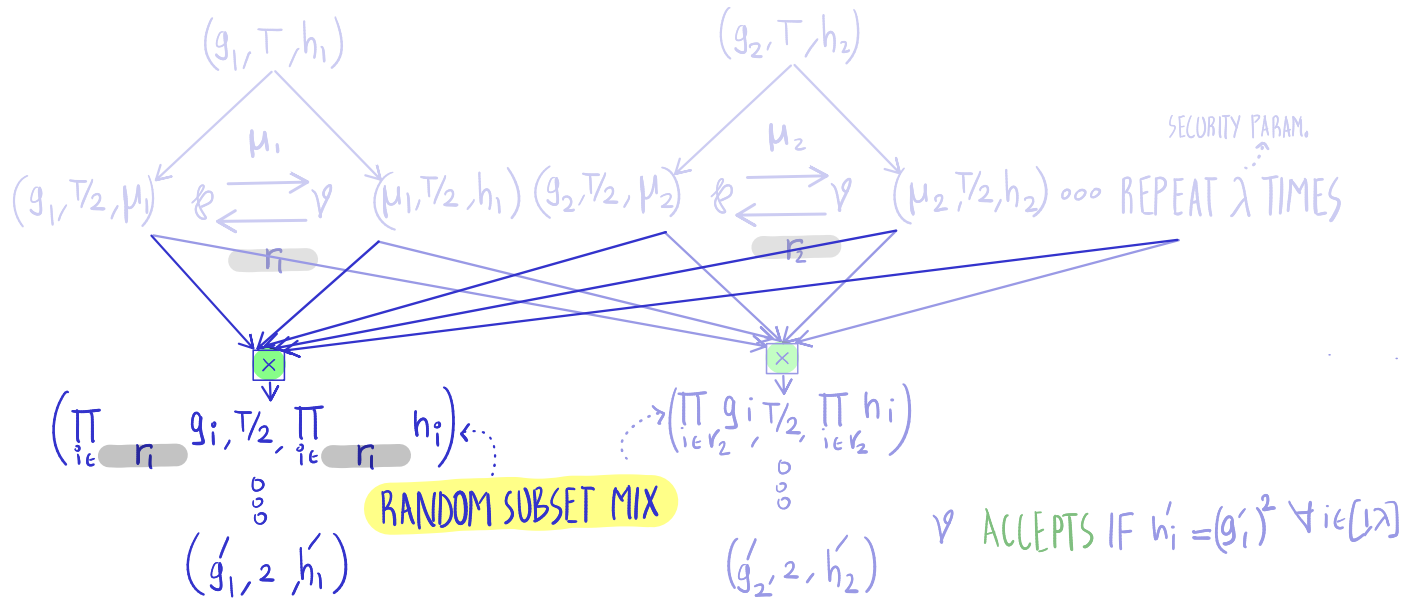
SOUND ?

FIAT-SHAMIR ?

\forall ACCEPTS IF $h'_i = (g'_i)^2 \forall i \in [1, \lambda]$

++ NI-ARG FOR $\mathcal{L}_{IS} \triangleq \{(g, T, h) : g^2 = h\}$

OUR SOLUTION: MIX THE REPETITIONS! [BHRRSZ1]



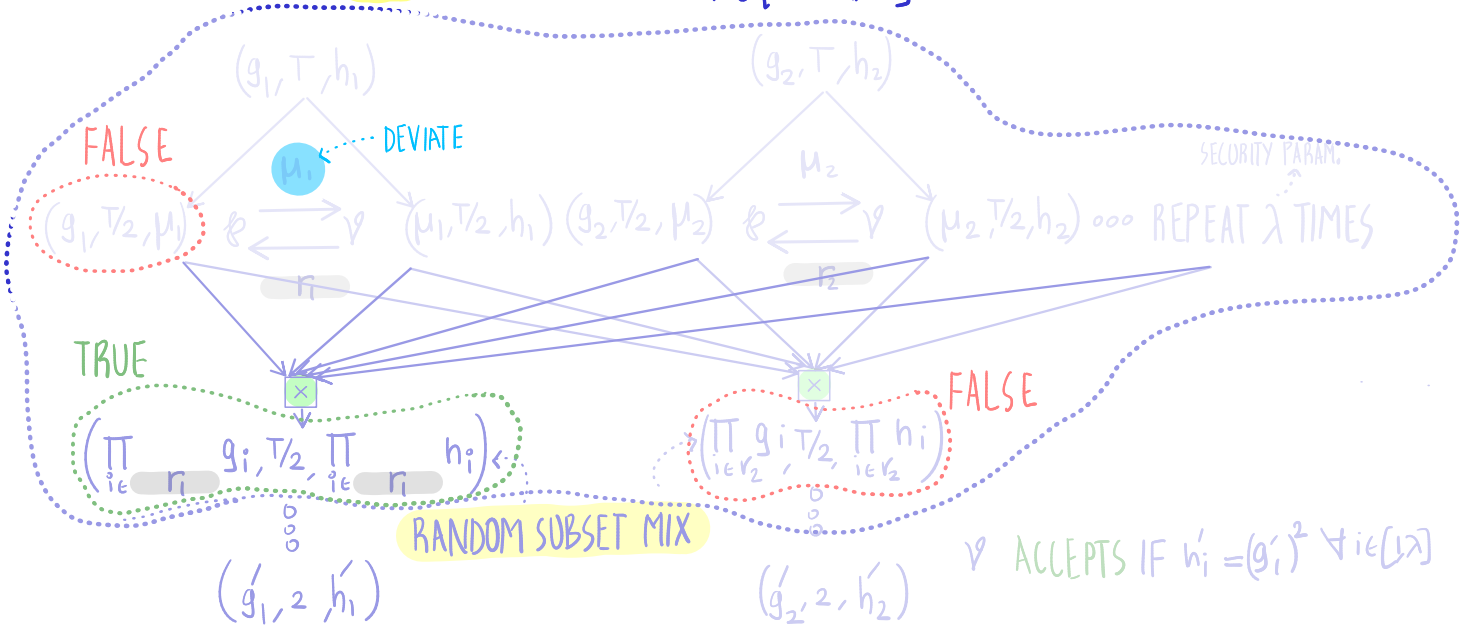
+UNIQUE ?

SOUND ? ~PARALLEL AMPLIFICATION: SEE [BHRRSZ1]

FIAT-SHAMIR ?

++ NI-ARG FOR $\mathcal{L}_{IS} \triangleq \{(g, T, h) : g^{2^T} = h\}$

OUR SOLUTION: MIX THE REPETITIONS! [BHRRS21]



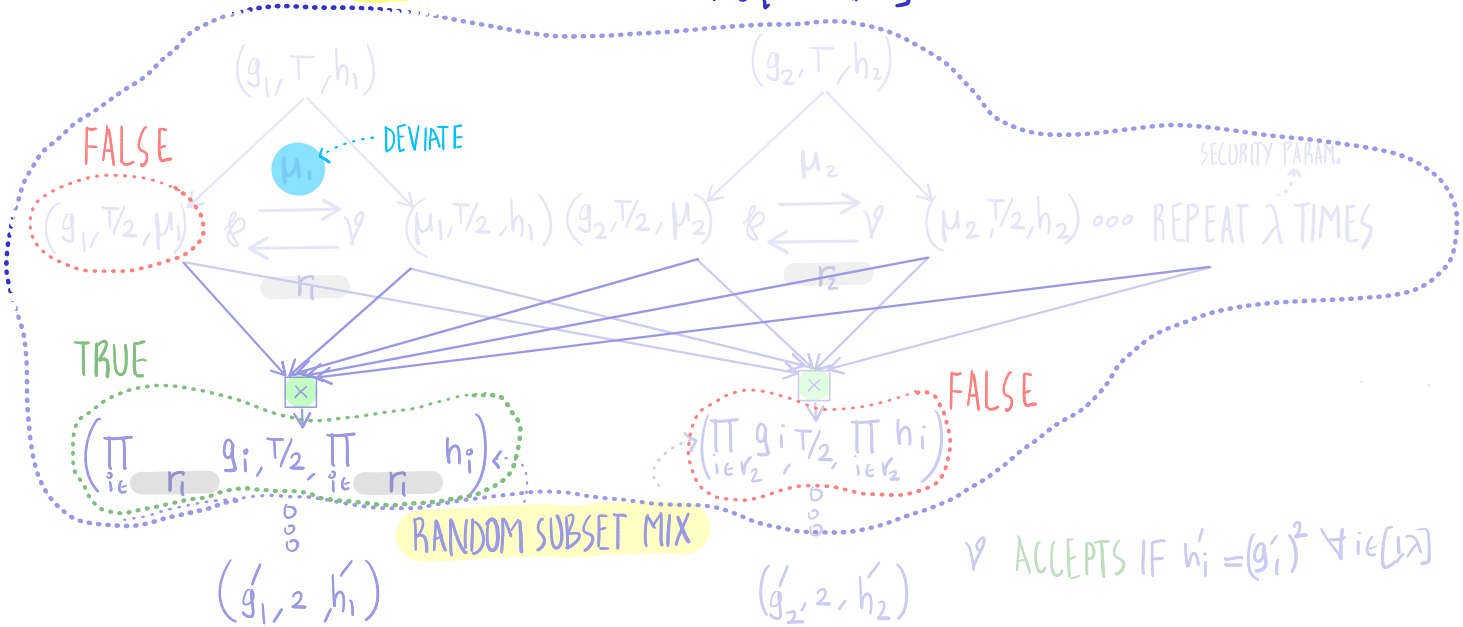
+UNIQUE? MIXING \Rightarrow DEVIATING LEADS TO \forall EVENTUALLY REJECTING

SOUND? \sim PARALLEL AMPLIFICATION: SEE [BHRRS21]

FIAT-SHAMIR?

++ NI-ARG FOR $\mathcal{L}_{IS} \triangleq \{(g, T, h) : g^{2^T} = h\}$

OUR SOLUTION: MIX THE REPETITIONS! [BHRRS21]



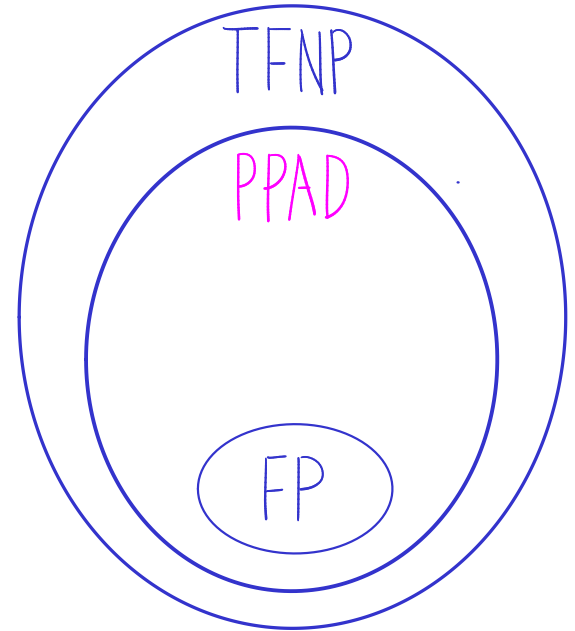
+UNIQUE? MIXING \Rightarrow DEVIATING LEADS TO \forall EVENTUALLY REJECTING

SOUND? \sim PARALLEL AMPLIFICATION: SEE [BHRRS21]

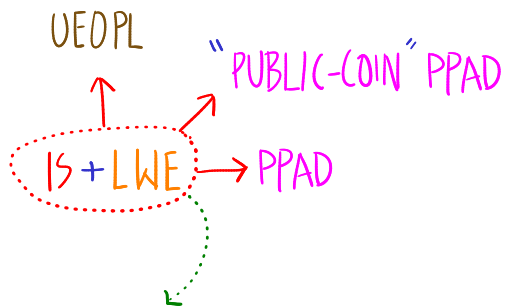
FIAT-SHAMIR? [HLR2] HASH FROM LWE

IN CONCLUSION...

IS + LWE \rightarrow PPAD

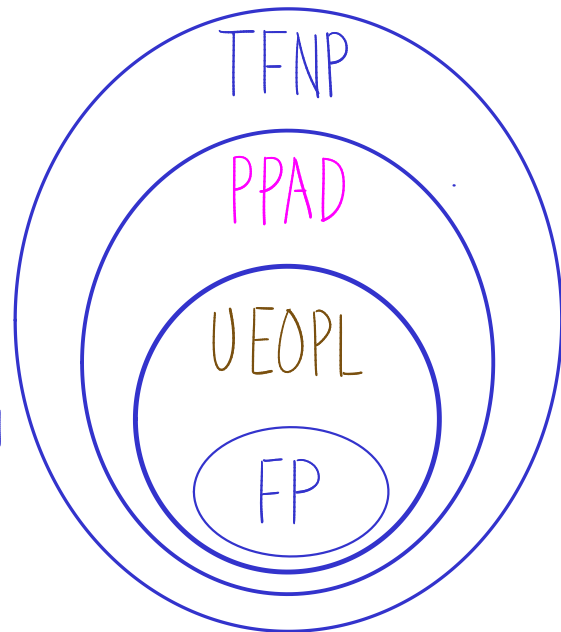


IN CONCLUSION...

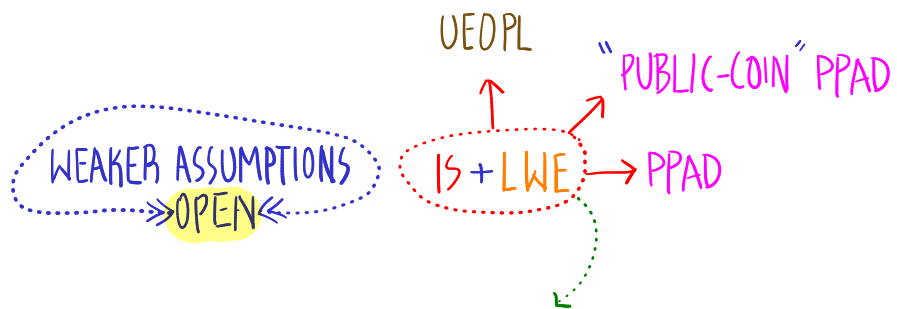


ABSTRACT BATCH-AND-OUTLINE PROTOCOL

CAPTURES PREVIOUS WORKS: [CHKPRR19_{a/b}, EFKP19, LV20, JKKZ21]

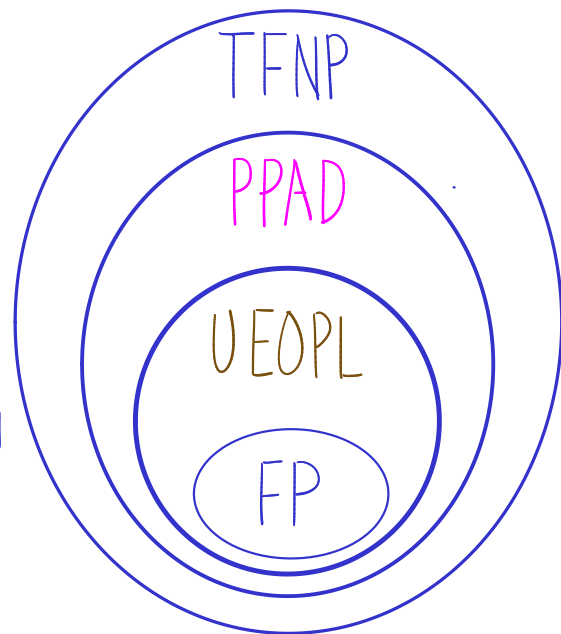


IN CONCLUSION...

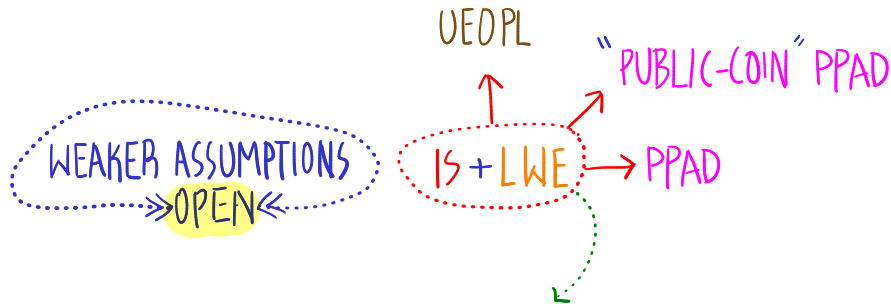


ABSTRACT BATCH-AND-OUTLINE PROTOCOL

CAPTURES PREVIOUS WORKS: [CHKPRR19_{a/b}, EFKP19, LV20, JKKZ21]

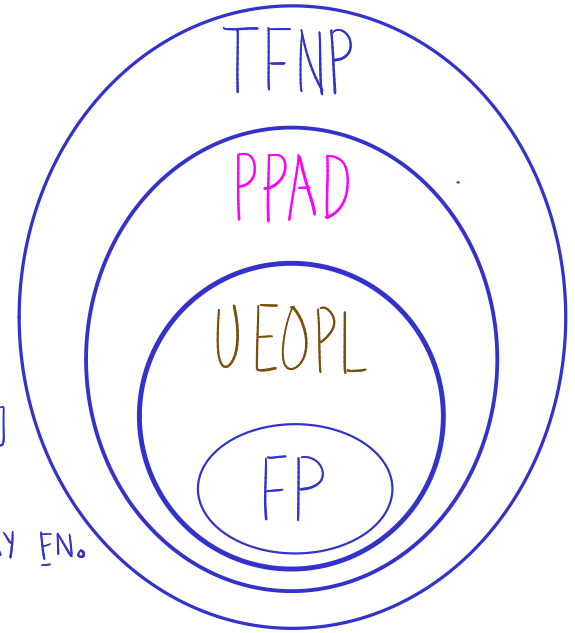
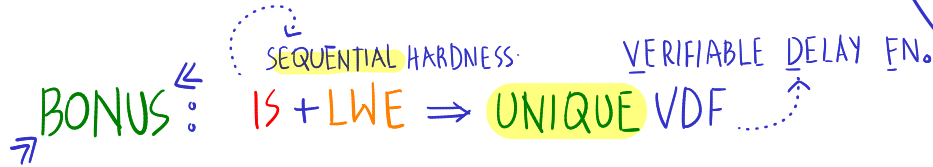


IN CONCLUSION...

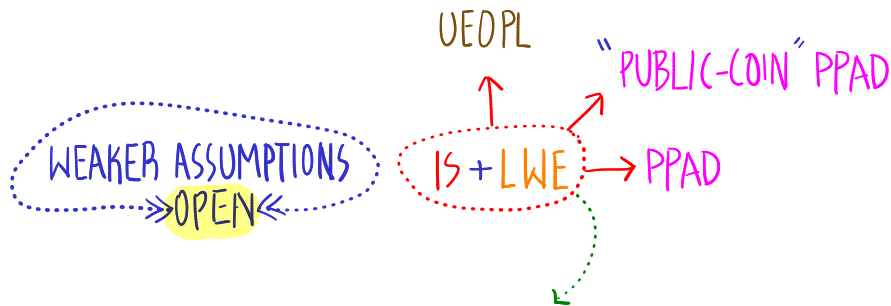


ABSTRACT BATCH-AND-OUTLINE PROTOCOL

CAPTURES PREVIOUS WORKS: [CHKPRR19a/b, EFKP19, LV20, JKKZ21]

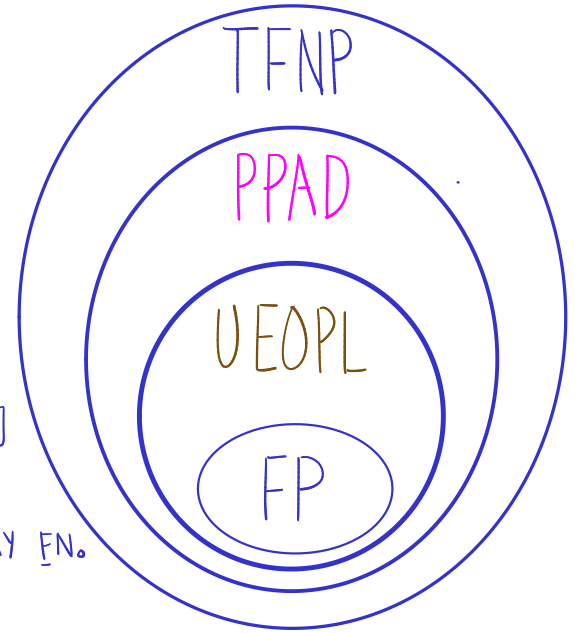


IN CONCLUSION...



ABSTRACT BATCH-AND-OUTLINE PROTOCOL

CAPTURES PREVIOUS WORKS: [CHKPRR19a/b, EFKP19, LV20, JKKZ21]



SEQUENTIAL HARDNESS

VERIFIABLE DELAY FN.

BONUS: IS + LWE ⇒ UNIQUE VDF

NEXT TALK: ANY SEQUENTIAL HARD FN. + LWE ⇒ VDF

THANK YOU!

THANK YOU! is written in a bubbly, hand-drawn font on a yellow cloud-like background. Each letter has a vertical word written next to it:

- T: TZETZ
- H: HAS
- A: HAS
- N: FISHAMIR
- K: ASSUMPTIO
- Y: STES
- O: PROPS
- U: LISON
- !: PEOPLE



תוכנית עמיתי עזריאלי
Azrieli Fellows Program

REFERENCES

BPR15 : BITANSKY, PANETH & ROSEN, ON THE CRYPTOGRAPHIC HARDNESS OF FINDING A NASH EQUILIBRIUM, FOCS 2015

BHRRS21 : BLOCK ET AL., TIME- & SPACE-EFFICIENT ARGUMENTS FROM GUD, CRYPTO 2021

CHKPRR19a : CHOUDHURI ET AL., FINDING A NASH EQUILIBRIUM IS NO EASIER THAN BREAKING FIAT-SHAMIR, STOC 2019

CHKPRR19b : —, PPAD-HARDNESS VIA IS MODULO A COMPOSITE, EPRINT 2019/667

EFKP19 : EPHRAIM ET AL., CONTINUOUS VDFs, EUROCRYPT 2020

GPS16 : GARG, PANDEY & SRINIVASAN, REVISITING THE CRYPTOGRAPHIC HARDNESS OF FINDING A NASH EQUILIBRIUM, CRYPTO 2016

HLR21 : HOLMGREN, LOMBARDI & ROTHBLUM, FIAT-SHAMIR VIA LIST RECOVERABLE CODES, STOC 2021

HY17 : HUBÁČEK & YOGEV, HARDNESS OF CONTINUOUS LOCAL SEARCH, SODA 2017

REFERENCES₀₀₀

- JKK21 : JAWALE ET AL., SNARGs FOR BOUNDED-DEPTH COMPUTATIONS & PPAD HARDNESS FROM SUB-EXP LWE, STOC 2021
- JLS21a : JAIN, LIN & SAHAI, IO FROM LPN OVER \mathbb{F}_p , DLIN AND PRGs IN \mathbb{N}° , EPRINT 2021/1334
- JLS21b : JAIN, LIN & SAHAI, IO FROM WELL-FOUNDED ASSUMPTIONS, STOC 2021
- LV20 : LOMBARDI & VAIKUNTANATHAN, FIAT-SHAMIR FOR REPEATED SQUARING WITH APPLICATIONS TO PPAD HARDNESS & VDFs, CRYPTO 2020
- PI9 : PIETRZAK, SIMPLE VDFs, ITCS 2019
- PS19 : PEIKERT & SHIEHIAN, NIZK FOR NP FROM (PLAIN) LWE, CRYPTO 2019
- RR16 : REINGOLD & ROTHBLUMs, CONSTANT-ROUND IPs FOR DELEGATING COMPUTATION, STOC 2016