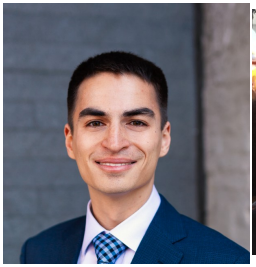
PPAD IS AS HARD AS LWE & ITERATED SQUARING

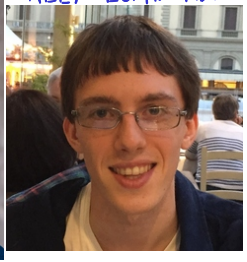
NIR BITANSKY

ARKA RAI CHOUDHURI

JUSTIN HOLMGREN



ALEX LOMBARDI



OMER PANETH

RON ROTHBLUM

CHETHAN KAMATH

NTT RESEARCH

TEL AVIV UNIVERSITY

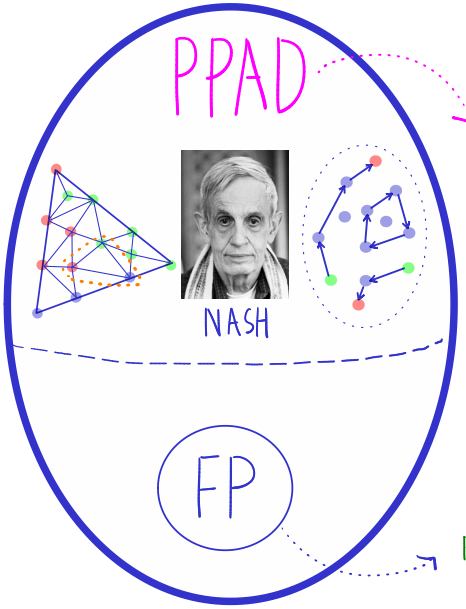
TECHNION

BERKELEY

SIMONS INSTITUTE

TCC 2022, NOV. 6-10, CHICAGO

PPAD

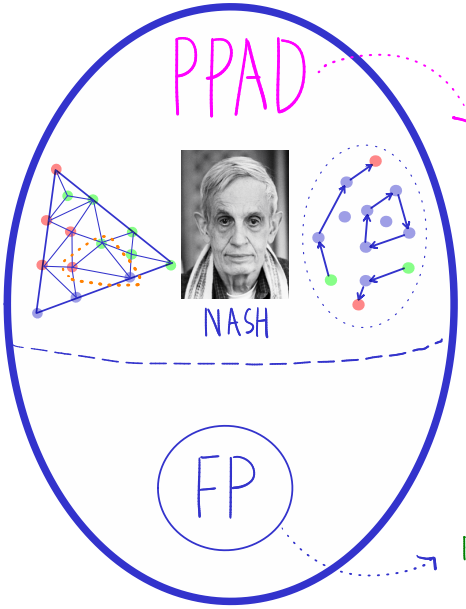


POLY. PARITY ARGUMENT ON DIGRAPHS

- CLASS OF SEARCH PROBLEMS

EASY SEARCH PROBLEMS

PPAD



POLY. PARITY ARGUMENT ON DIGRAPHS

- CLASS OF SEARCH PROBLEMS

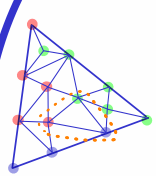
EASY SEARCH PROBLEMS

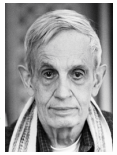
CRYPTO $\overset{?}{\rightarrow}$ PPAD IS HARD

PPAD ⊆ TFNP

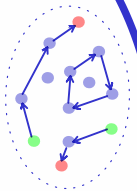
TOTAL FUNCTIONAL NP

PPAD





NASH



POLY. PARITY ARGUMENT ON DIGRAPHS

- CLASS OF SEARCH PROBLEMS

FP

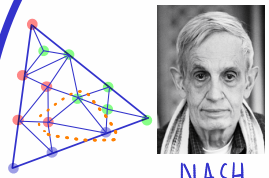
EASY SEARCH PROBLEMS

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

PPAD ⊆ TFNP

TOTAL FUNCTIONAL NP

PPAD



NASH

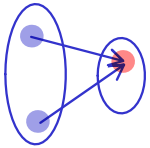
FP

POLY. PARITY ARGUMENT ON DIGRAPHS

- CLASS OF SEARCH PROBLEMS

- FACTOR
- COLLISION

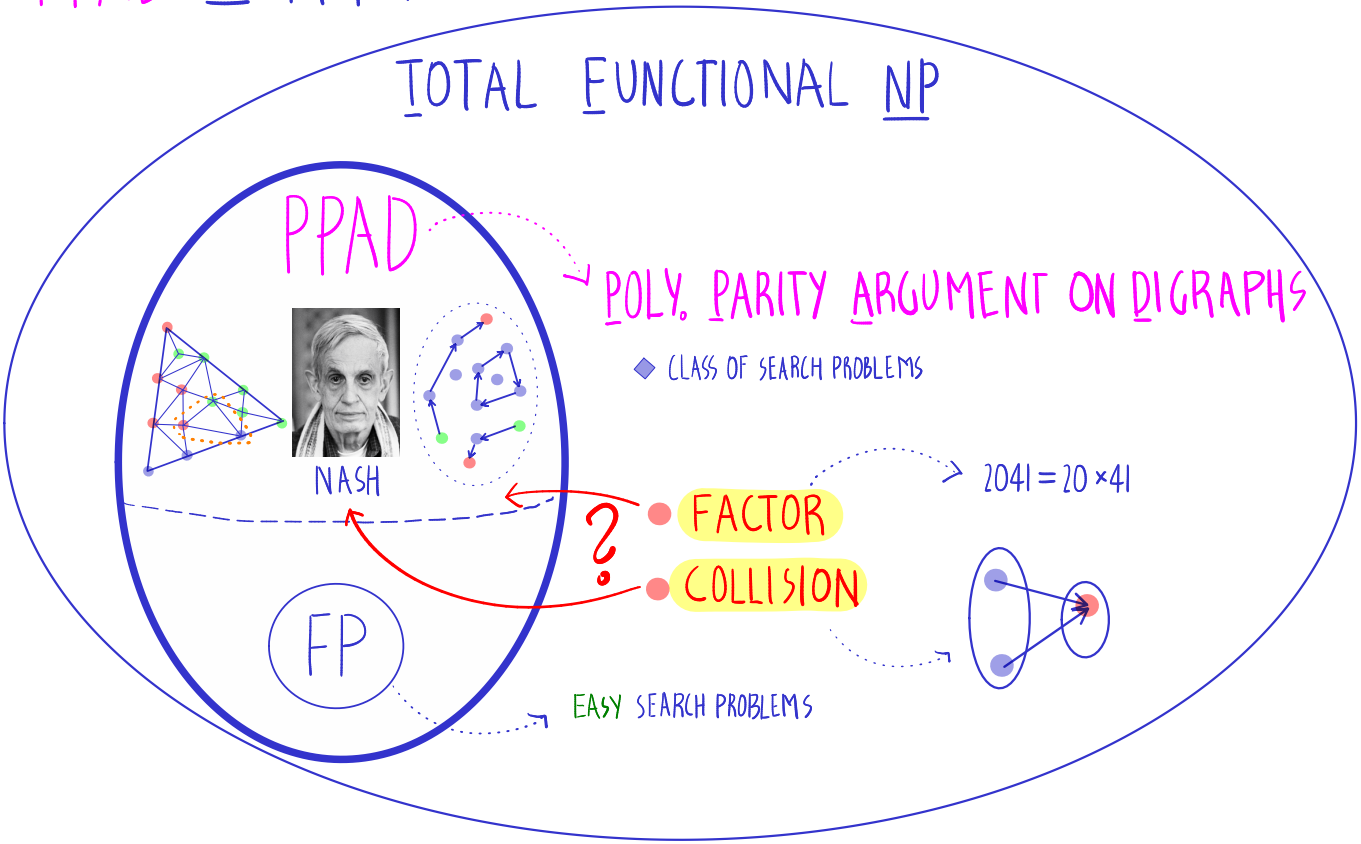
$2041 = 20 \times 41$



EASY SEARCH PROBLEMS

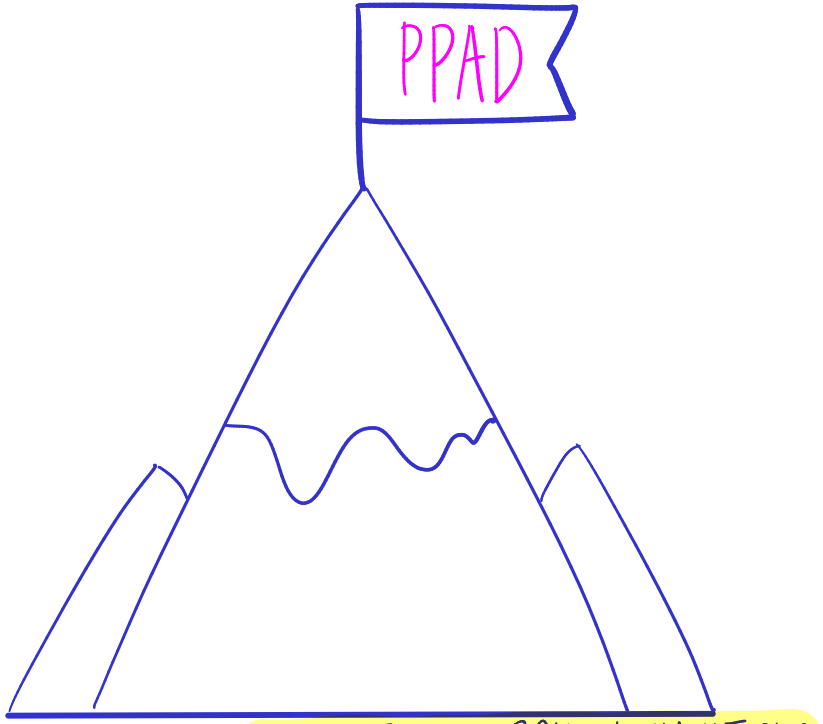
CRYPTO $\overset{?}{\rightarrow}$ PPAD IS HARD

PPAD ⊆ TFNP



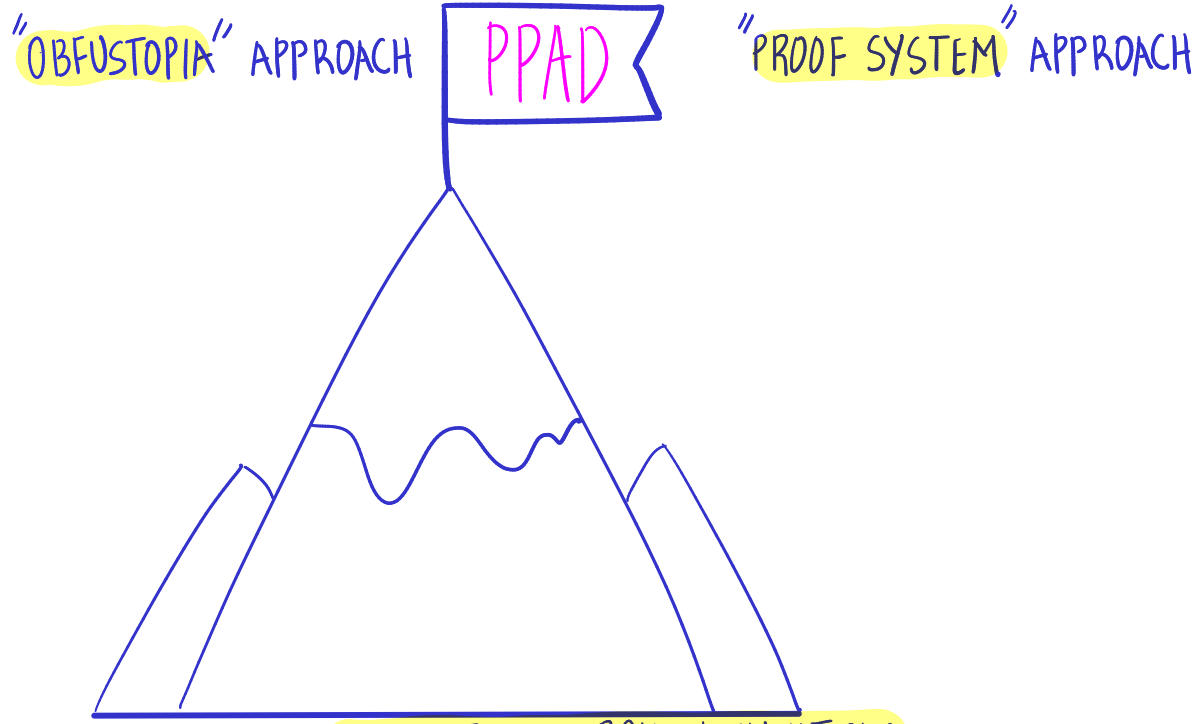
CRYPTO $\overset{?}{\rightarrow}$ PPAD IS HARD

CRYPTO $\Rightarrow$ PPAD IS HARD

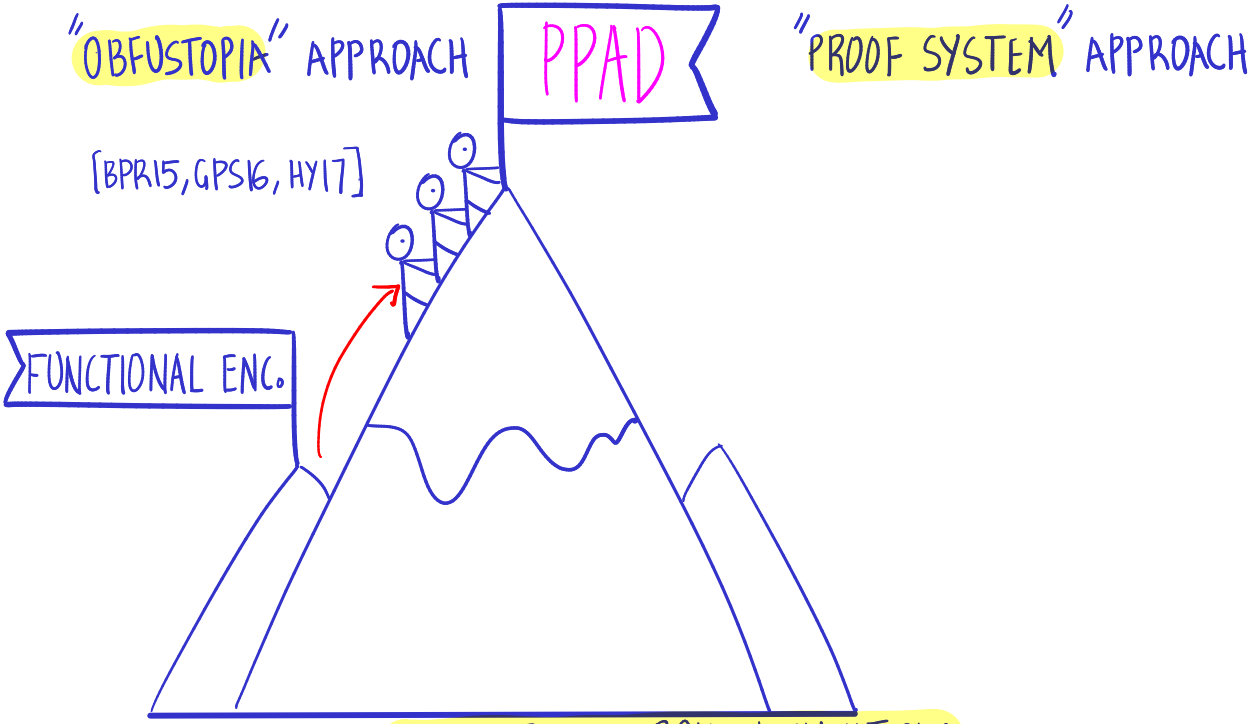


STANDARD CRYPTO : WELL-STUDIED, POLY. ASSUMPTIONS

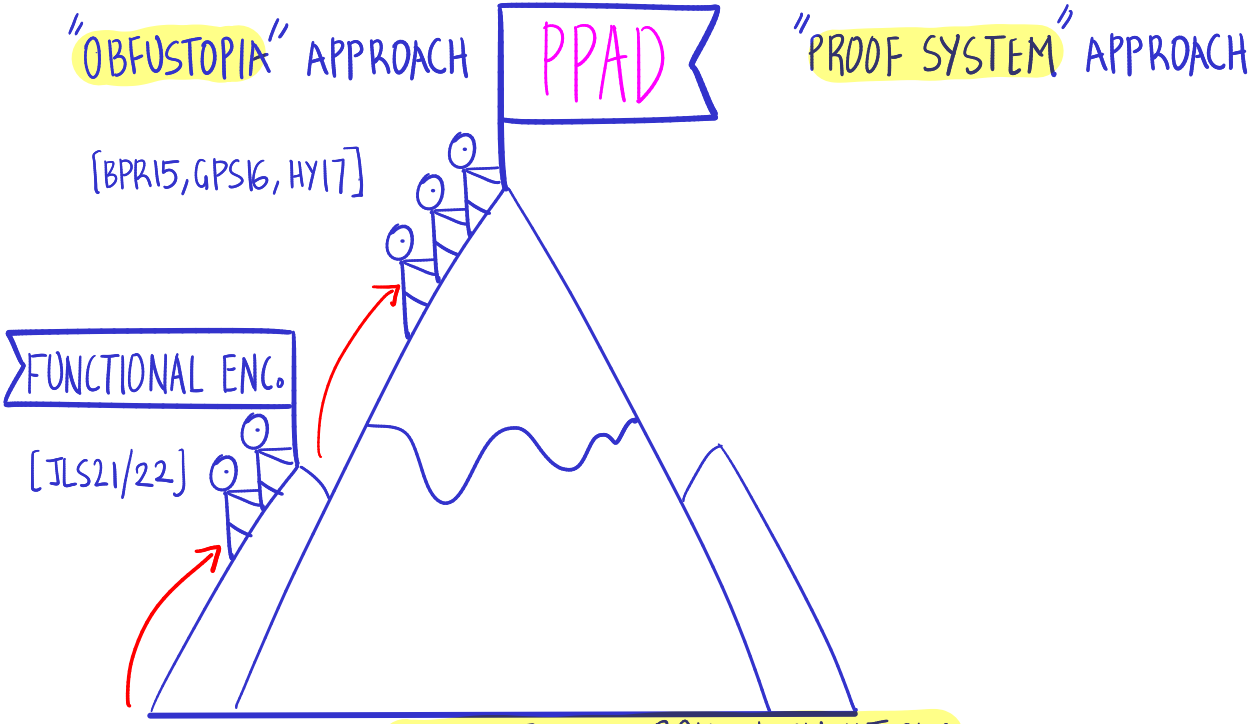
CRYPTO ⇒ PPAD IS HARD



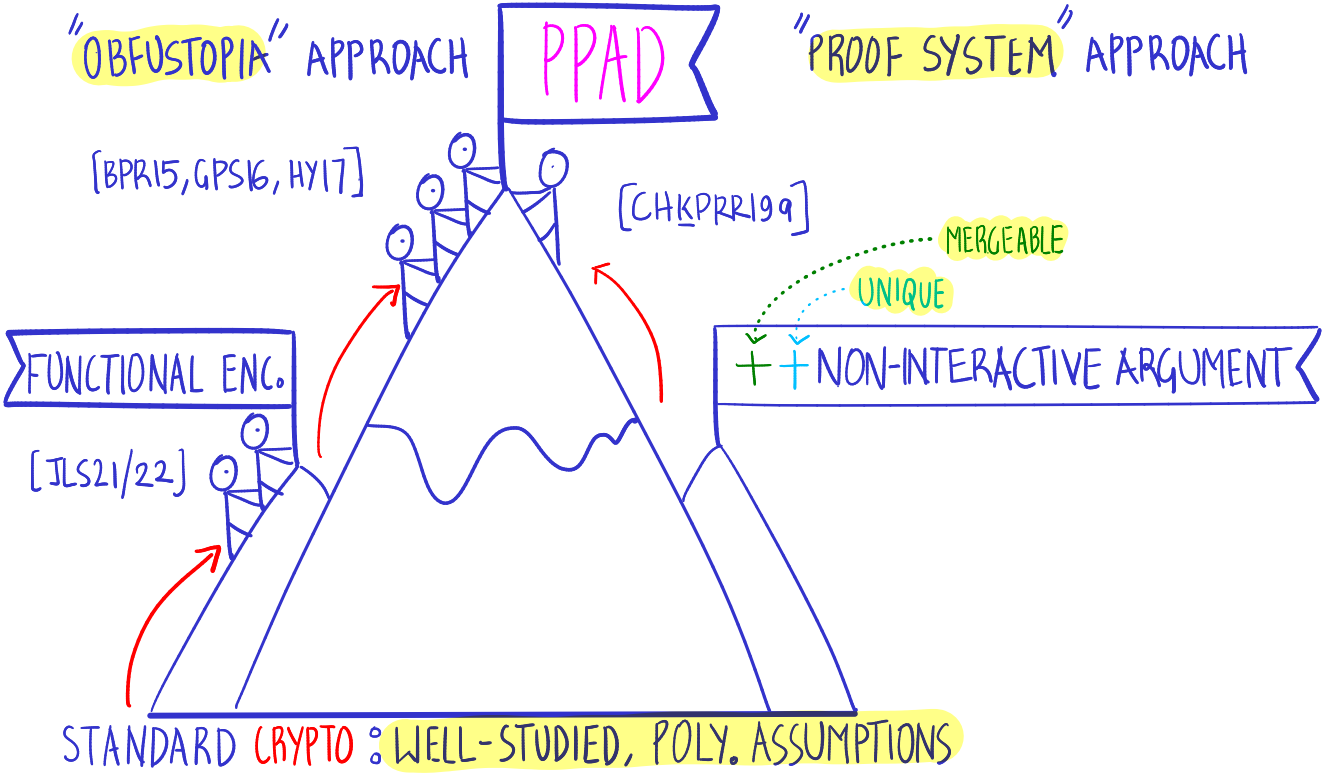
CRYPTO ⇒ PPAD IS HARD



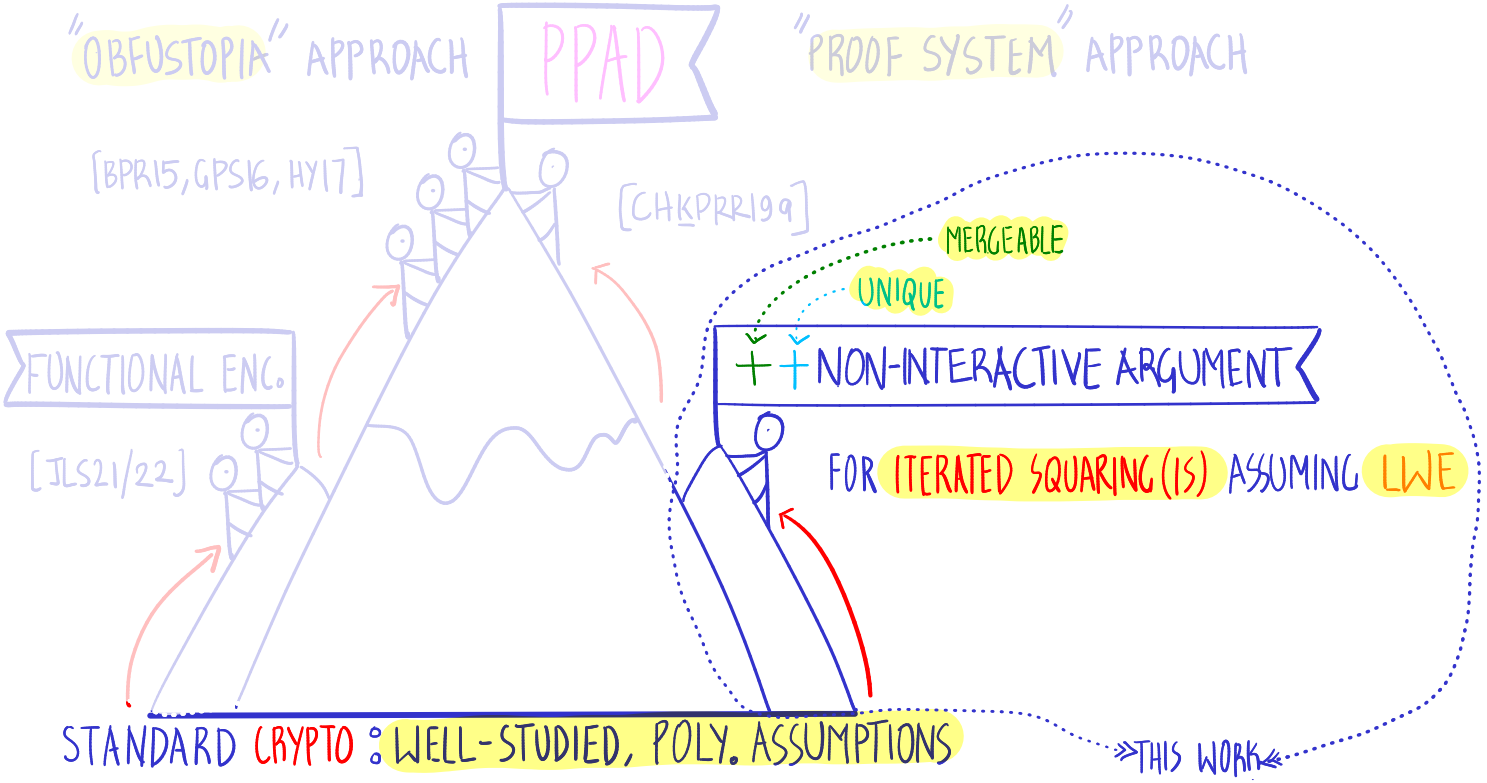
CRYPTO ⇒ PPAD IS HARD



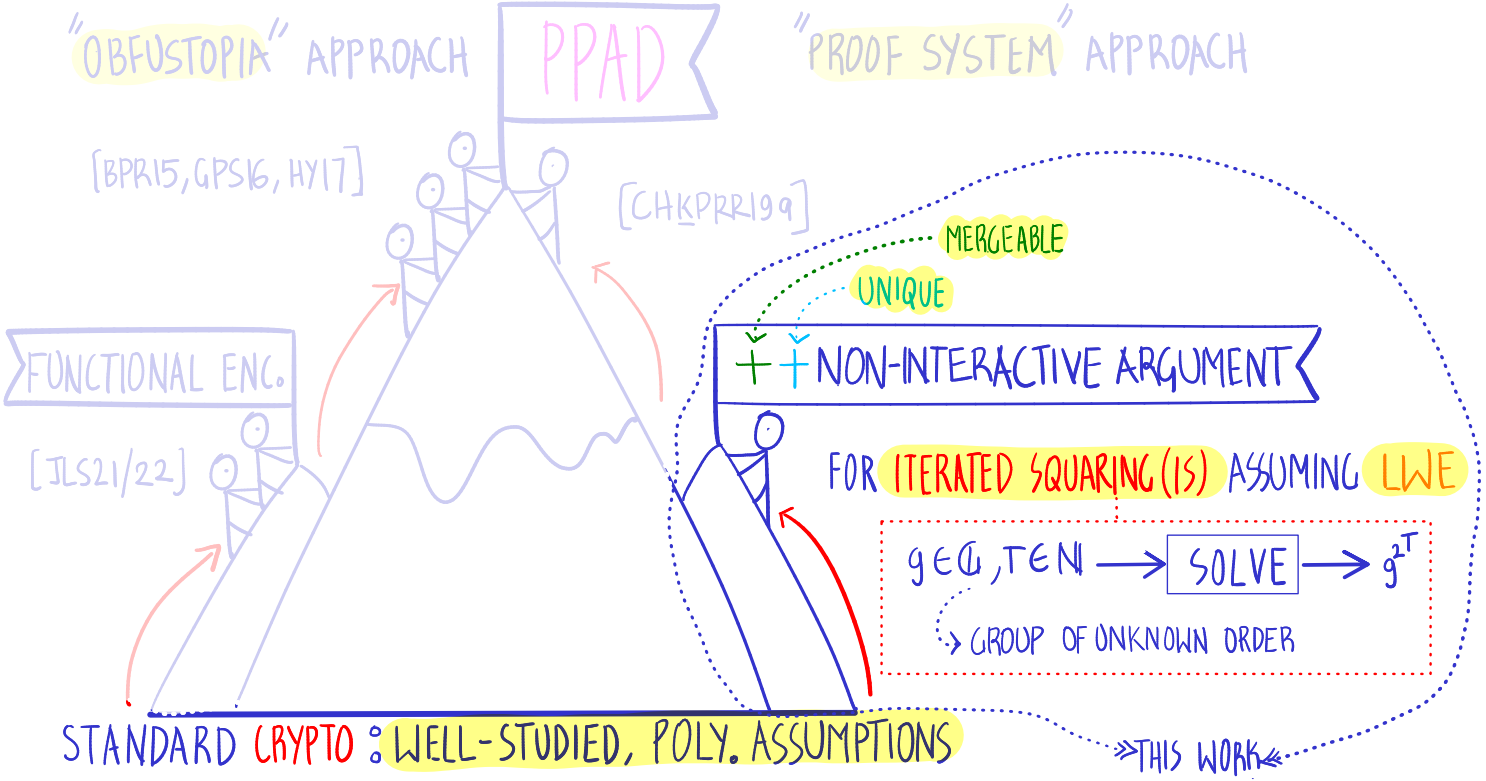
CRYPTO ⇒ PPAD IS HARD



CRYPTO ⇒ PPAD IS HARD

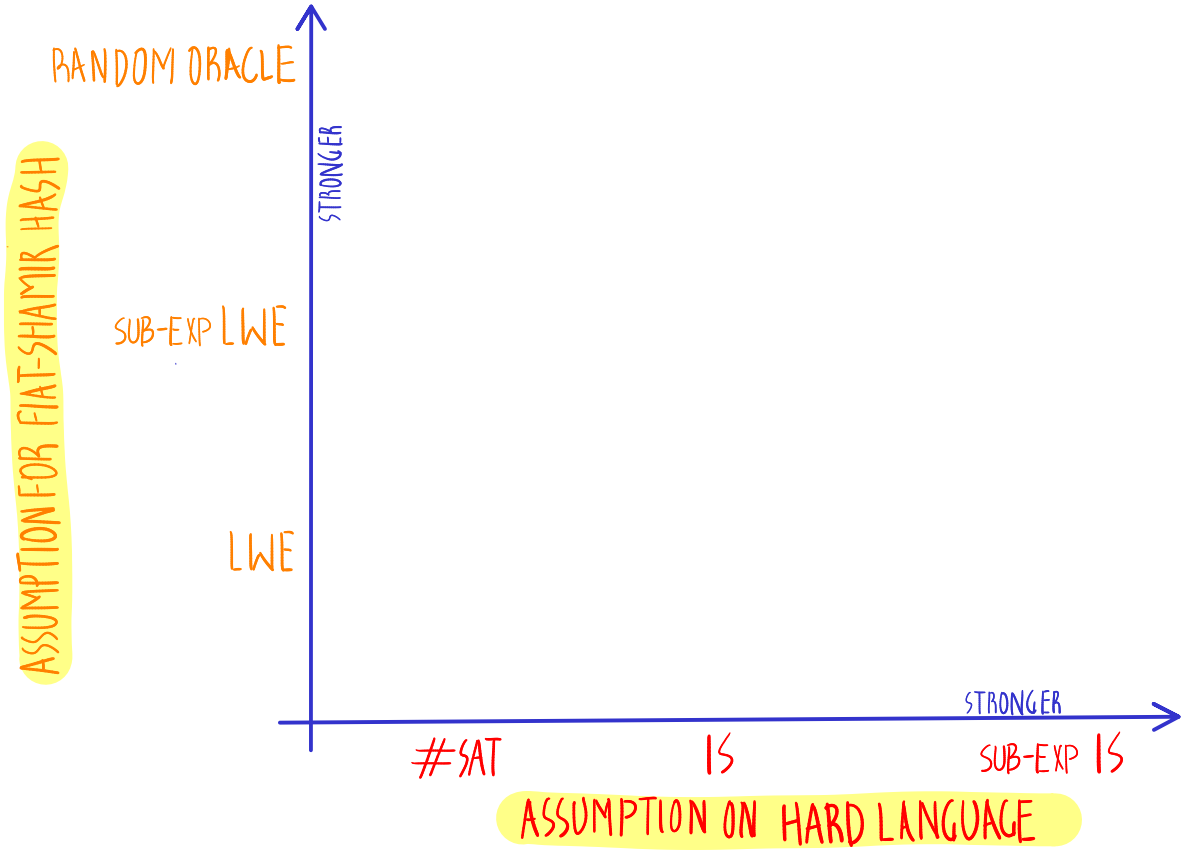


CRYPTO ⇒ PPAD IS HARD

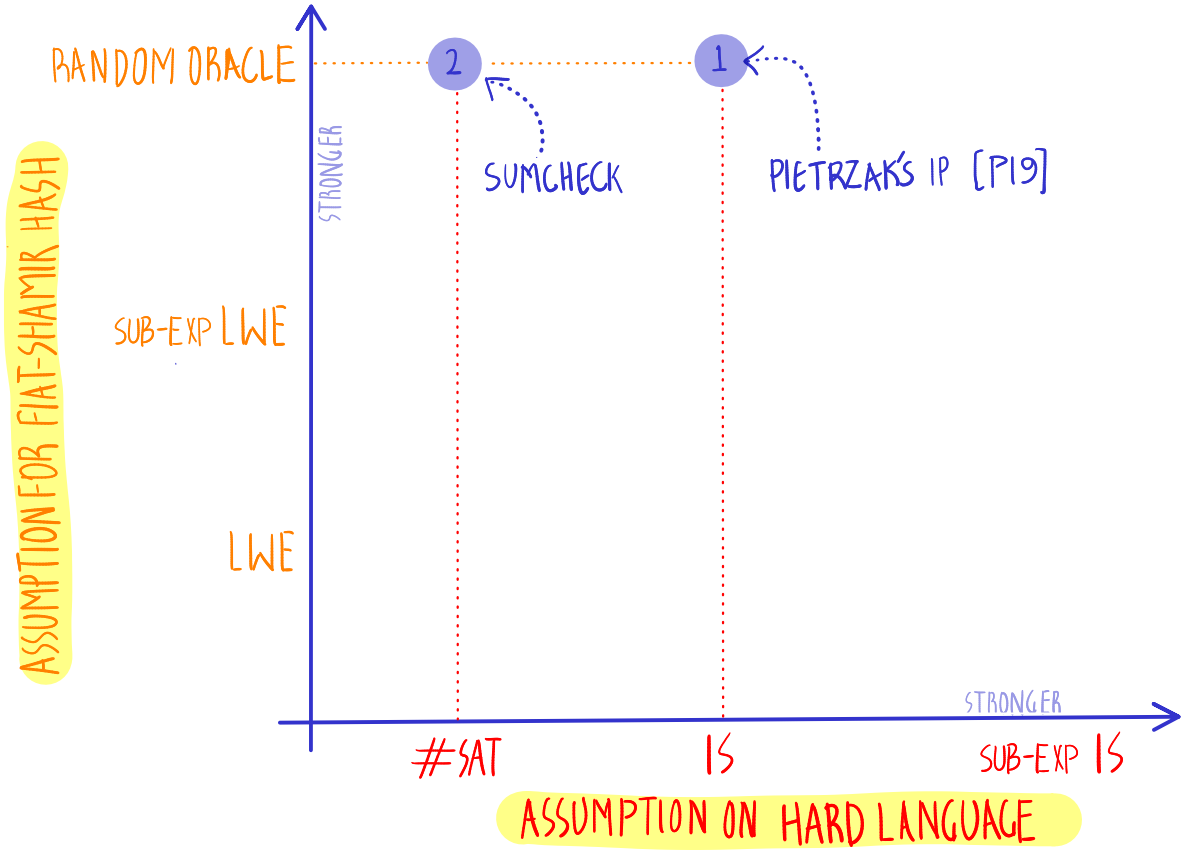


++IP FOR $\mathcal{L}$ $\xrightarrow{\text{FIAT-SHAMIR}}$ ++NI-ARG FOR $\mathcal{L}$

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

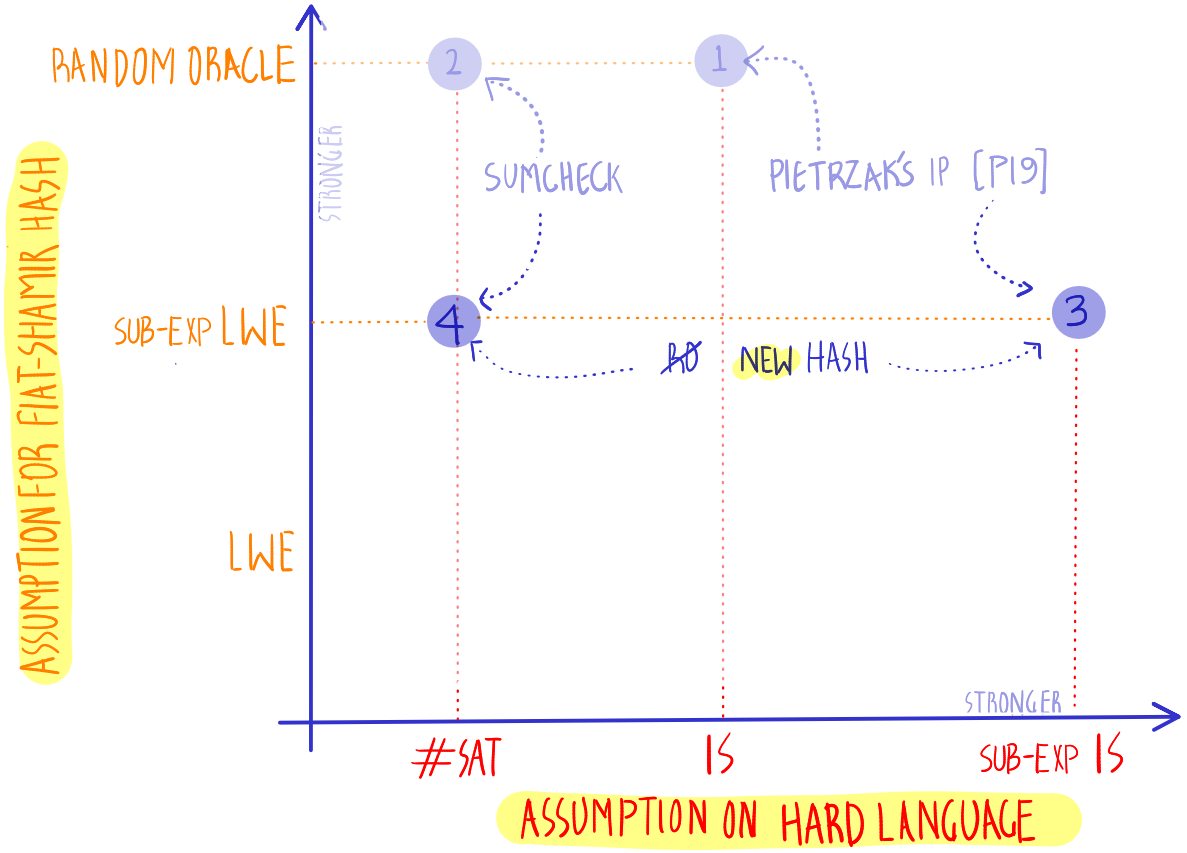


++IP FOR $\mathcal{L}$ $\xrightarrow{\text{FIAT-SHAMIR}}$ ++NI-ARG FOR $\mathcal{L}$



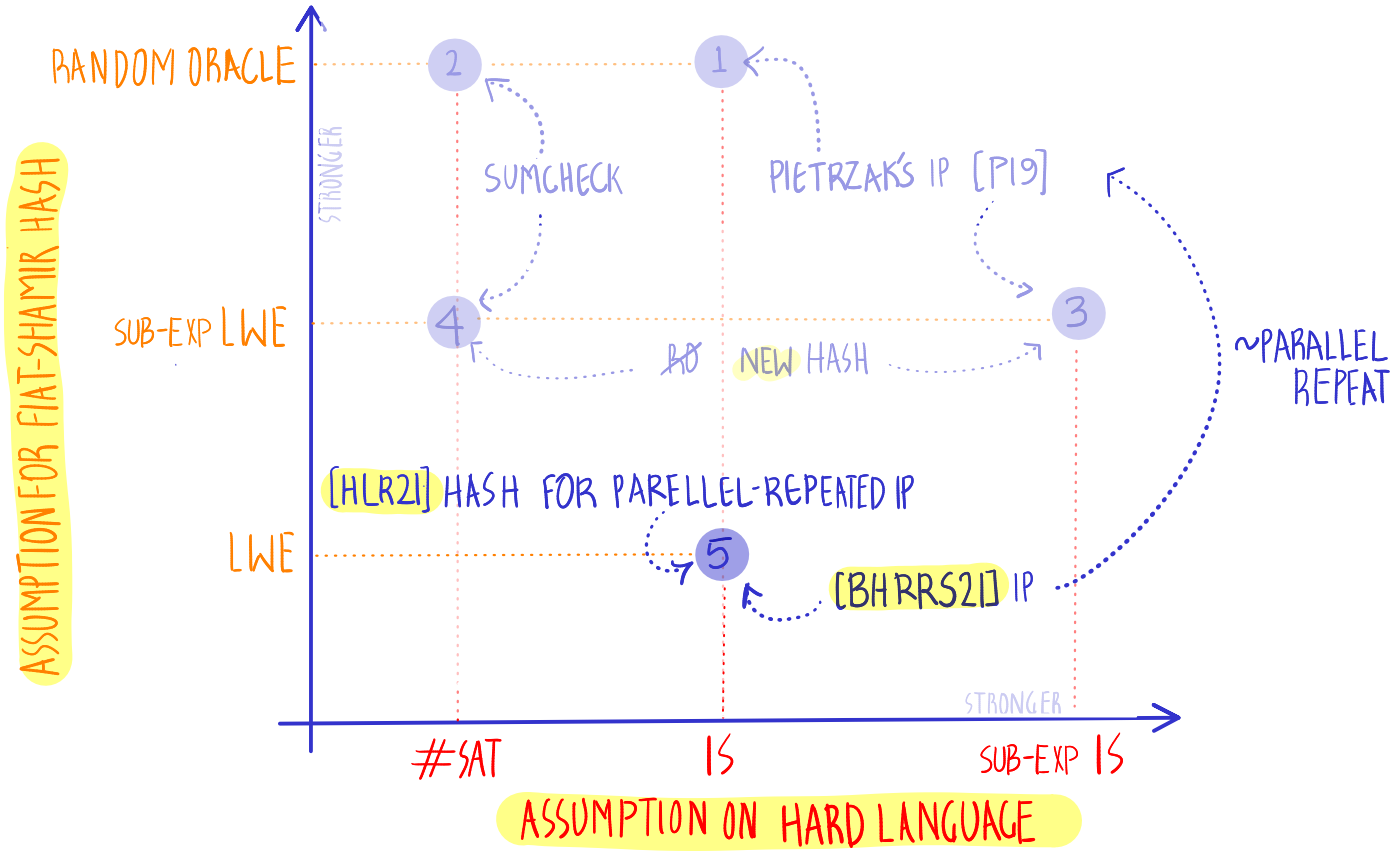
1 [CHKPRR19a, EFKP19] 2 [CHKPRR19b]

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



1 [CHKPRR19a, EFKP19] 2 [CHKPRR19b] 3 [LV20] 4 [JKKZ21]

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



1 [CHKPRR19a, EFKP19] 2 [CHKPRR19b] 3 [LV20] 4 [JKKZ21] 5 [THIS WORK]

++NI-ARG

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

ITERATED SQUARING (IS)

$g \in \mathbb{G}, T \in \mathbb{N} \rightarrow$ SOLVE $\rightarrow g^{2^T}$

$\mathbb{G}$ → GROUP OF UNKNOWN ORDER

$$g \xrightarrow{2} g^2 \xrightarrow{2} \cdots \xrightarrow{2} g^{2^{T/2}} \xrightarrow{2} g^{2^{T/2+1}} \xrightarrow{2} \cdots \xrightarrow{2} g^{2^T}$$

"MIDPOINT"

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

ITERATED SQUARING (IS)

$g \in \mathbb{G}, T \in \mathbb{N} \rightarrow$ SOLVE $\rightarrow g^{2^T}$

$\mathbb{G}$ → GROUP OF UNKNOWN ORDER

$$g \xrightarrow{2} g^2 \xrightarrow{2} \cdots \xrightarrow{2} g^{2^{T/2}} \xrightarrow{2} g^{2^{T/2+1}} \xrightarrow{2} \cdots \xrightarrow{2} g^{2^T}$$

"MIDPOINT"

+MERGEABLE

PROOFS OF SMALL RELATED STATEMENTS

↓

PROOF OF LARGER STATEMENT

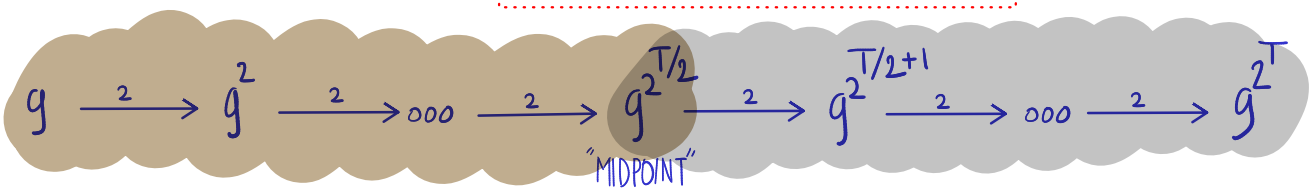
FASTER THAN COMPUTING FROM SCRATCH

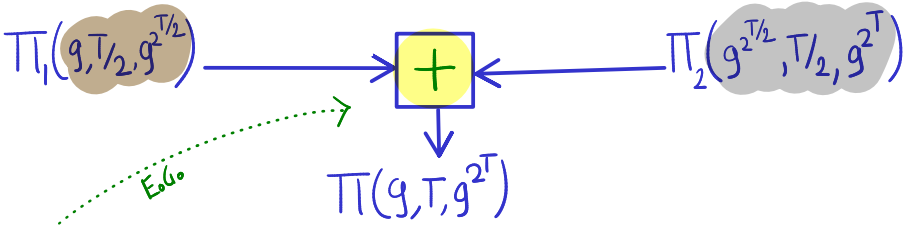
++NI-ARG FOR $\alpha_{IS} \triangleq \{(g,T,h) : g^{2^T} = h\}$

ITERATED SQUARING (IS)

$g \in \mathbb{G}, T \in \mathbb{N} \rightarrow$ SOLVE $\rightarrow g^{2^T}$

→ GROUP OF UNKNOWN ORDER





+ MERGEABLE

PROOFS OF SMALL RELATED STATEMENTS

↓

PROOF OF LARGER STATEMENT

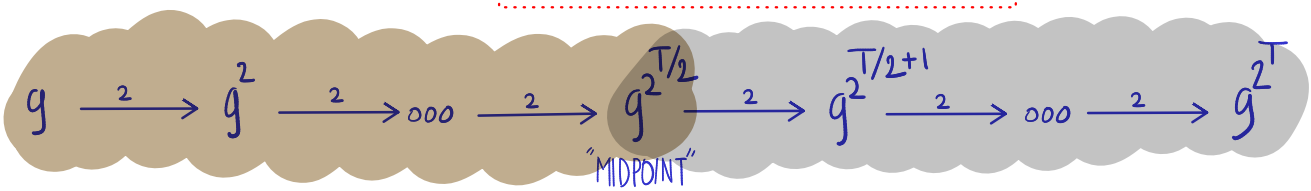
FASTER THAN COMPUTING FROM SCRATCH

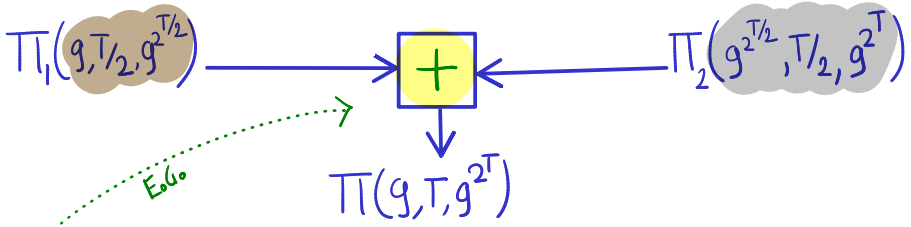
++NI-ARG FOR $\mathcal{L}_{IS} \triangleq \{(g,T,h) : g^{2^T} = h\}$

ITERATED SQUARING (IS)

$g \in \mathbb{G}, T \in \mathbb{N} \rightarrow$ SOLVE $\rightarrow g^{2^T}$

→ GROUP OF UNKNOWN ORDER





+ MERGEABLE

PROOFS OF SMALL RELATED STATEMENTS

↓

PROOF OF LARGER STATEMENT

FASTER THAN COMPUTING FROM SCRATCH

+ UNIQUE

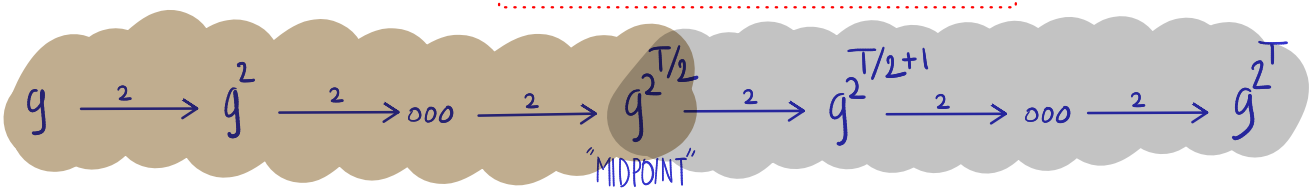
HARD TO FIND TWO PROOFS FOR A TRUE STATEMENT

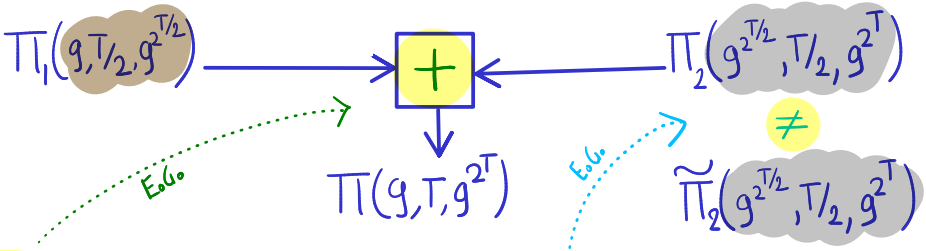
++NI-ARG FOR $\alpha_{IS} \triangleq \{(g,T,h) : g^{2^T} = h\}$

ITERATED SQUARING (IS)

$g \in \mathbb{G}, T \in \mathbb{N} \rightarrow$ SOLVE $\rightarrow g^{2^T}$

→ GROUP OF UNKNOWN ORDER





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

ITERATED SQUARING (IS)

$g \in \mathbb{G}, T \in \mathbb{N} \rightarrow$ SOLVE $\rightarrow g^{2^T}$

$\rightarrow$ GROUP OF UNKNOWN ORDER

$g \xrightarrow{2} g^2 \xrightarrow{2} \cdots \xrightarrow{2} g^{2^{T/2}} \xrightarrow{2} g^{2^{T/2+1}} \xrightarrow{2} \cdots \xrightarrow{2} g^{2^T}$

"MIDPOINT"

$\Pi_1(g, T/2, g^{2^{T/2}}) \rightarrow +$

$\Pi_2(g^{2^{T/2}}, T/2, g^{2^T}) \rightarrow +$

$+ \rightarrow \Pi(g, T, g^{2^T})$

$\Pi_2(g^{2^{T/2}}, T/2, g^{2^T}) \neq \widetilde{\Pi}_2(g^{2^{T/2}}, T/2, g^{2^T})$

E.G.

+ MERGEABLE

PROOFS OF SMALL RELATED STATEMENTS

$\downarrow$

PROOF OF LARGER STATEMENT

FASTER THAN COMPUTING FROM SCRATCH

E.G.

+ UNIQUE

HARD TO FIND TWO PROOFS FOR A TRUE STATEMENT

$\gg$ FOCUS $\ll$

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

ATTEMPT 1: PIETRZAK'S IP [P19]

+UNIQUE?

SOUND?

FIAT-SHAMIR?

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

ATTEMPT 1: PIETRZAK'S IP [P19]

(g, T, h)

$\mathcal{P}$ $\mathcal{V}$

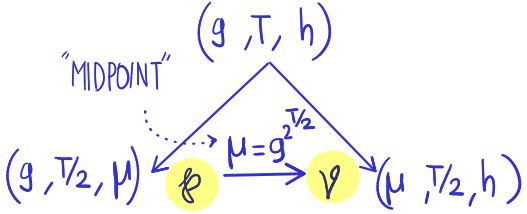
+UNIQUE?

SOUND?

FIAT-SHAMIR?

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

ATTEMPT 1: PIETRZAK'S IP [P19]



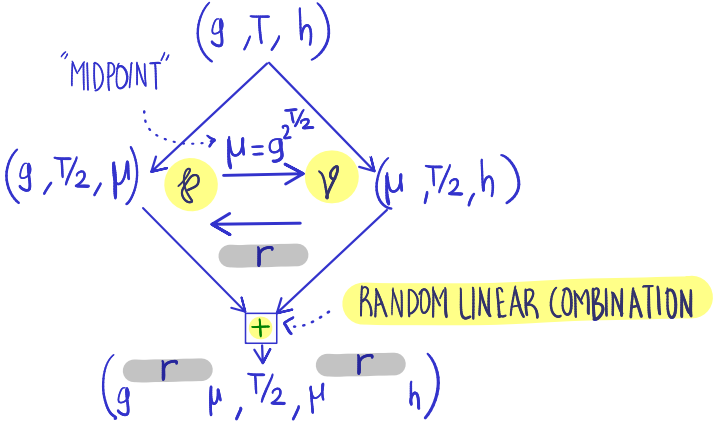
+UNIQUE?

SOUND?

FIAT-SHAMIR?

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

ATTEMPT 1: PIETRZAK'S IP [P19]



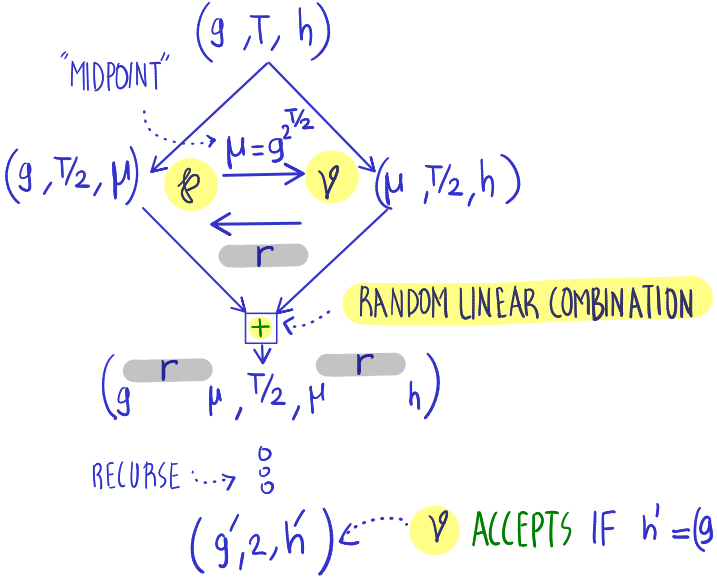
+UNIQUE?

SOUND?

FIAT-SHAMIR?

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

ATTEMPT 1: PIETRZAK'S IP [PI9]



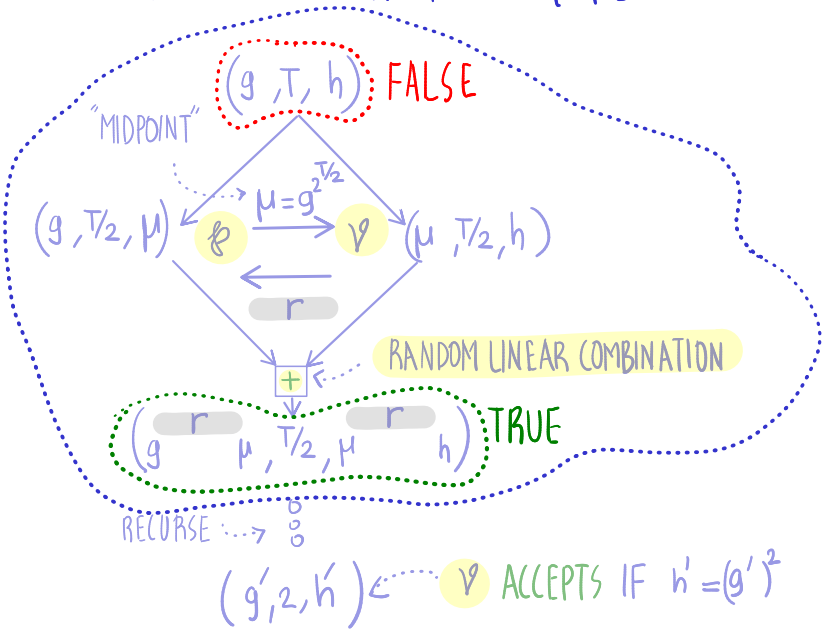
+UNIQUE?

SOUND?

FIAT-SHAMIR?

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

ATTEMPT 1: PIETRZAK'S IP [PI9]



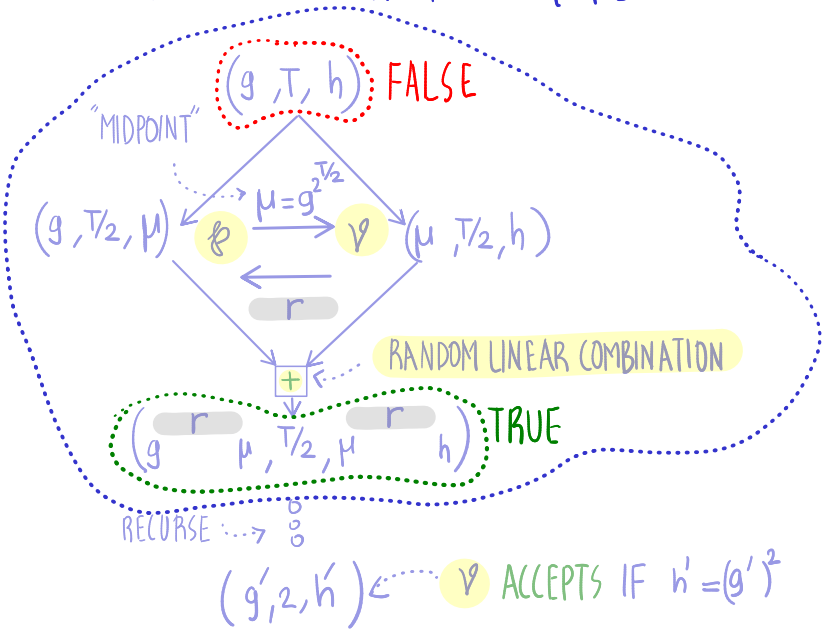
+UNIQUE?

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

FIAT-SHAMIR?

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

ATTEMPT 1: PIETRZAK'S IP [PI19]



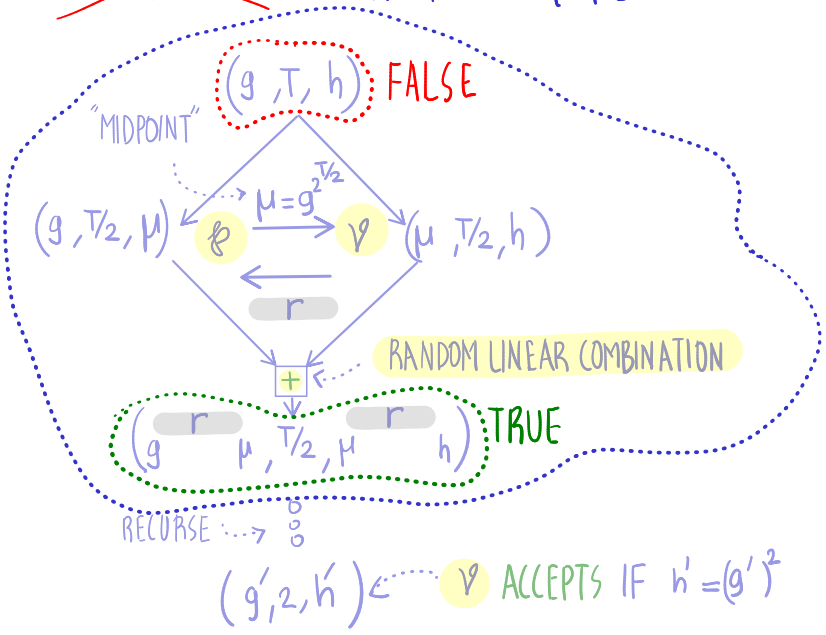
+UNIQUE?

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

FIAT-SHAMIR? ? SOLVE DLP $\Rightarrow$ CANNOT USE [PS19] HASH FROM LWE

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

~~ATTEMPT 1:~~ PIETRZAK's IP [P19]



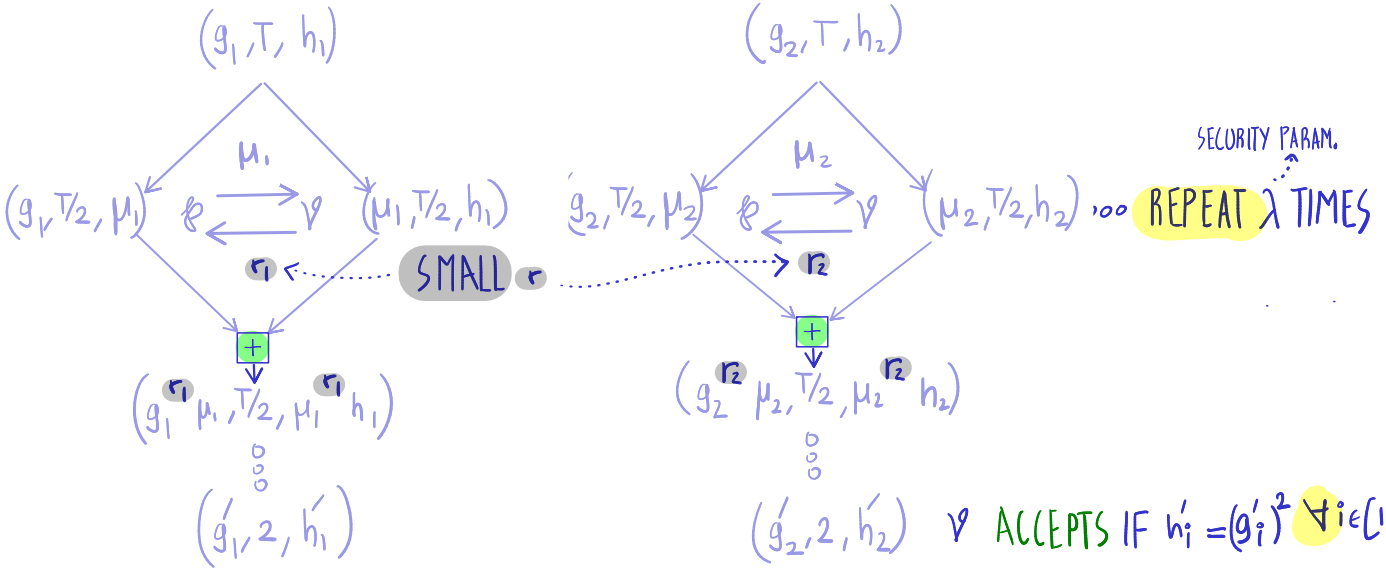
+UNIQUE?

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

FIAT-SHAMIR? ? SOLVE DLP $\Rightarrow$ CANNOT USE [PS19] 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



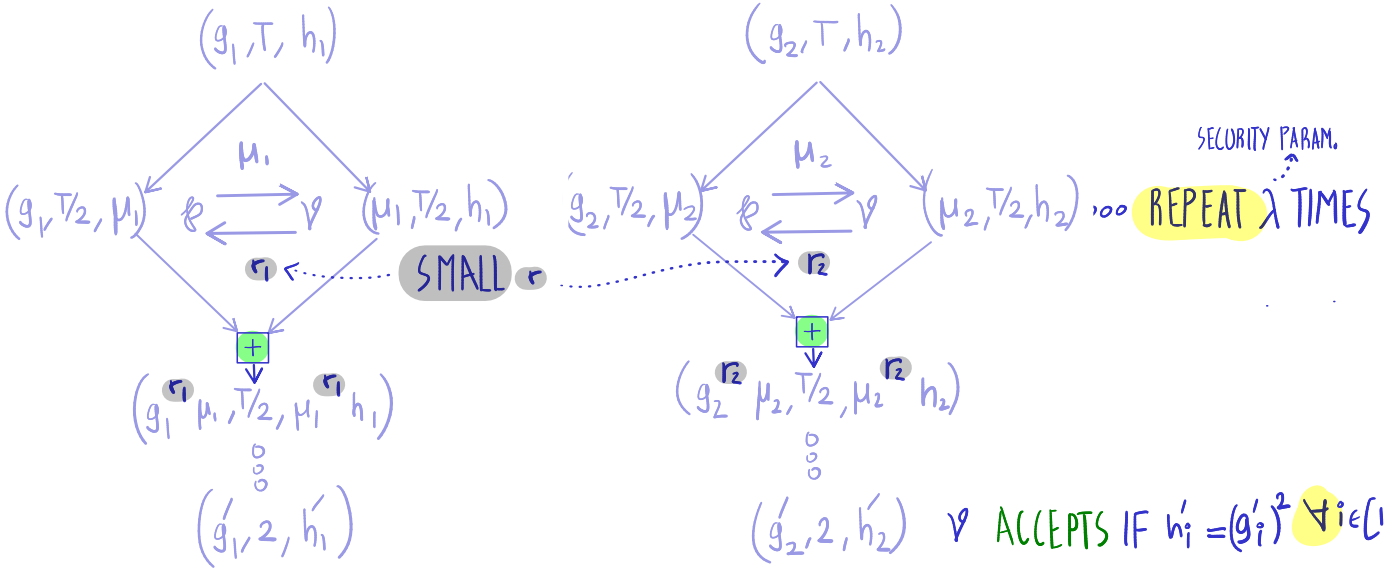
+UNIQUE ?

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



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

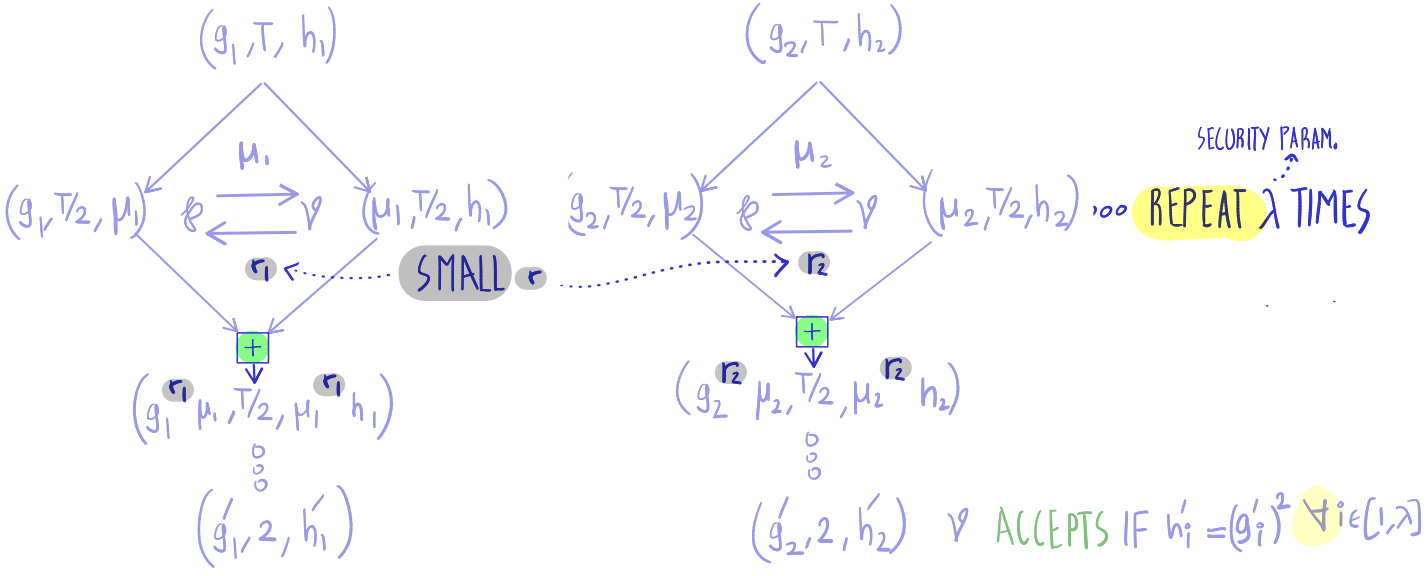
+UNIQUE ?

SOUND ? ✓ PARALLEL REP. AMPLIFIES SOUNDNESS

FIAT-SHAMIR ? ✓ [HLR21] HASH FOR PARELLEL-REPEATED IP 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



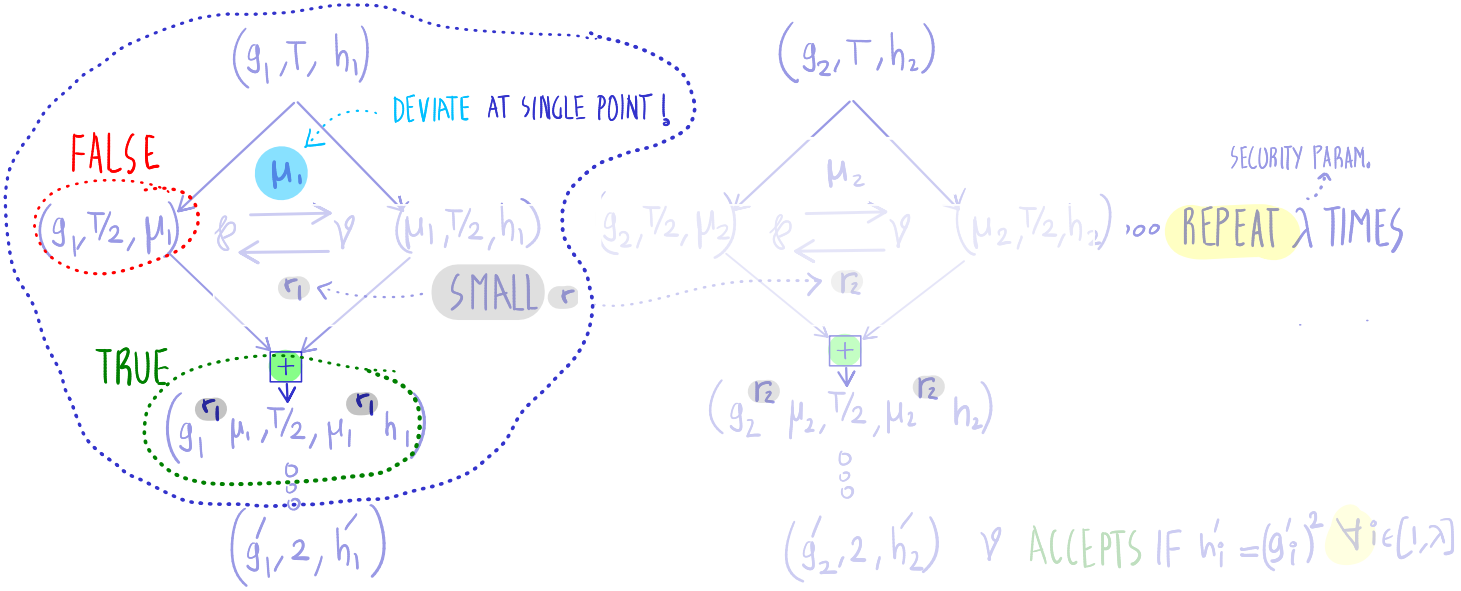
+UNIQUE? ✗ PARALLEL REP. DOESN'T PRESERVE UNIQUENESS! [RRR16]

SOUND? ✓ PARALLEL REP. AMPLIFIES SOUNDNESS

FIAT-SHAMIR? ✓ [HLR21] HASH FOR PARELLEL-REPEATED IP 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



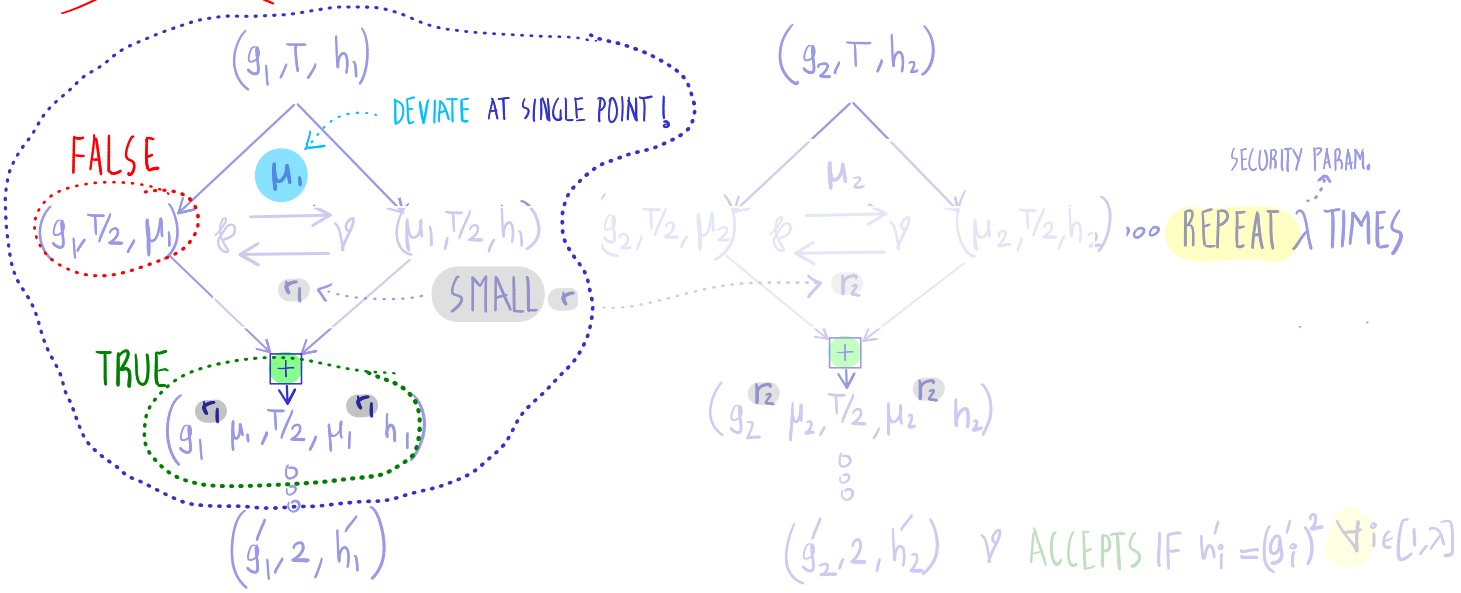
+UNIQUE? ✗ PARALLEL REP. DOESN'T PRESERVE UNIQUENESS! [RRR16]

SOUND? ✓ PARALLEL REP. AMPLIFIES SOUNDNESS

FIAT-SHAMIR? ✓ [HLR21] HASH FOR PARELLEL-REPEATED IP 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



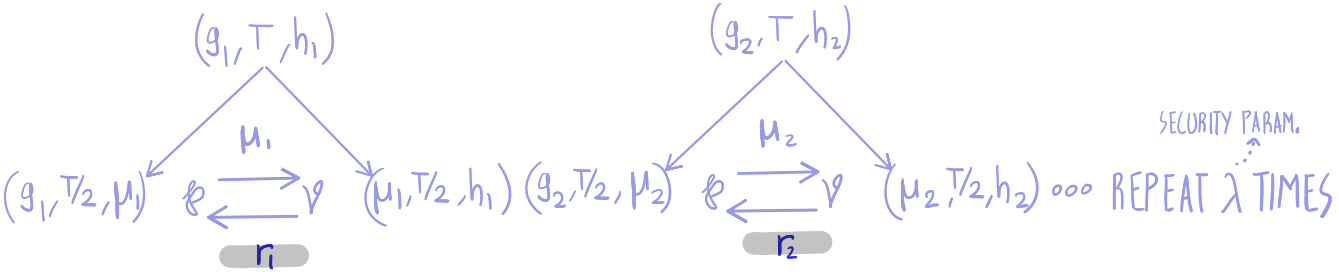
+UNIQUE? ✗ PARALLEL REP. DOESN'T PRESERVE UNIQUENESS! [RRR16]

SOUND? ✓ PARALLEL REP. AMPLIFIES SOUNDNESS

FIAT-SHAMIR? ✓ [HLR21] HASH FOR PARELLEL-REPEATED IP FROM LWE

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

OUR SOLUTION: MIX THE REPETITIONS! [BHRRS21]



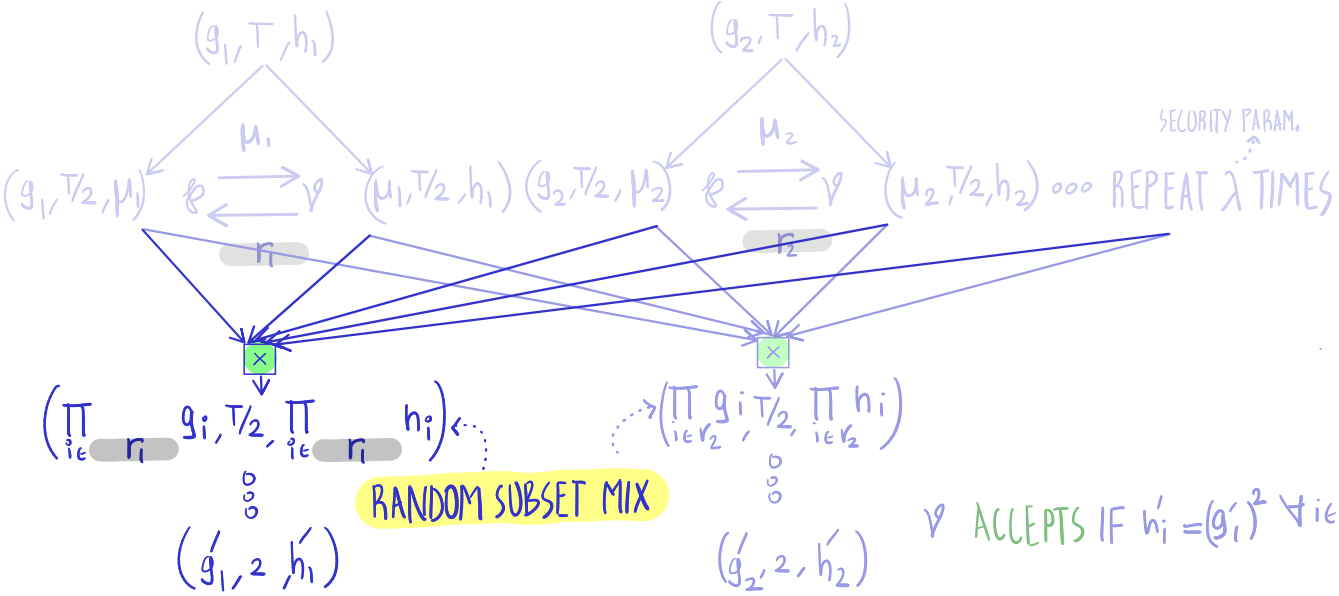
+UNIQUE ?

SOUND ?

FIAT-SHAMIR ?

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

OUR SOLUTION: MIX THE REPETITIONS! [BHRRS21]



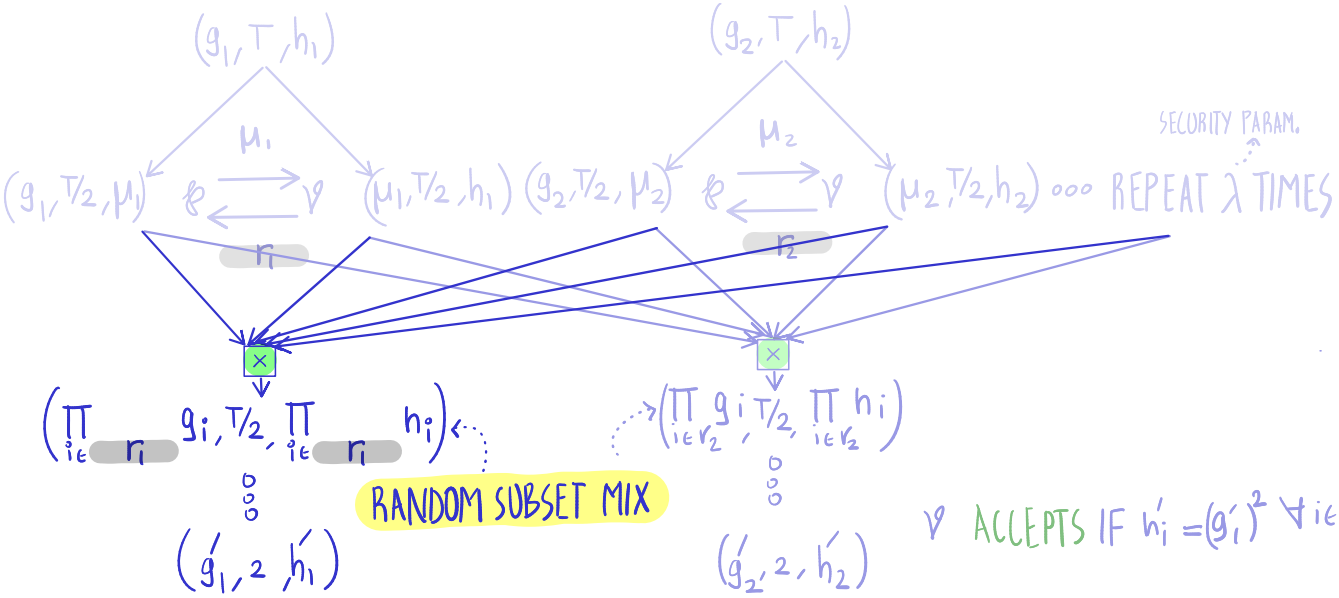
+UNIQUE?

SOUND?

FIAT-SHAMIR?

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

OUR SOLUTION: MIX THE REPETITIONS! [BHRRS21]



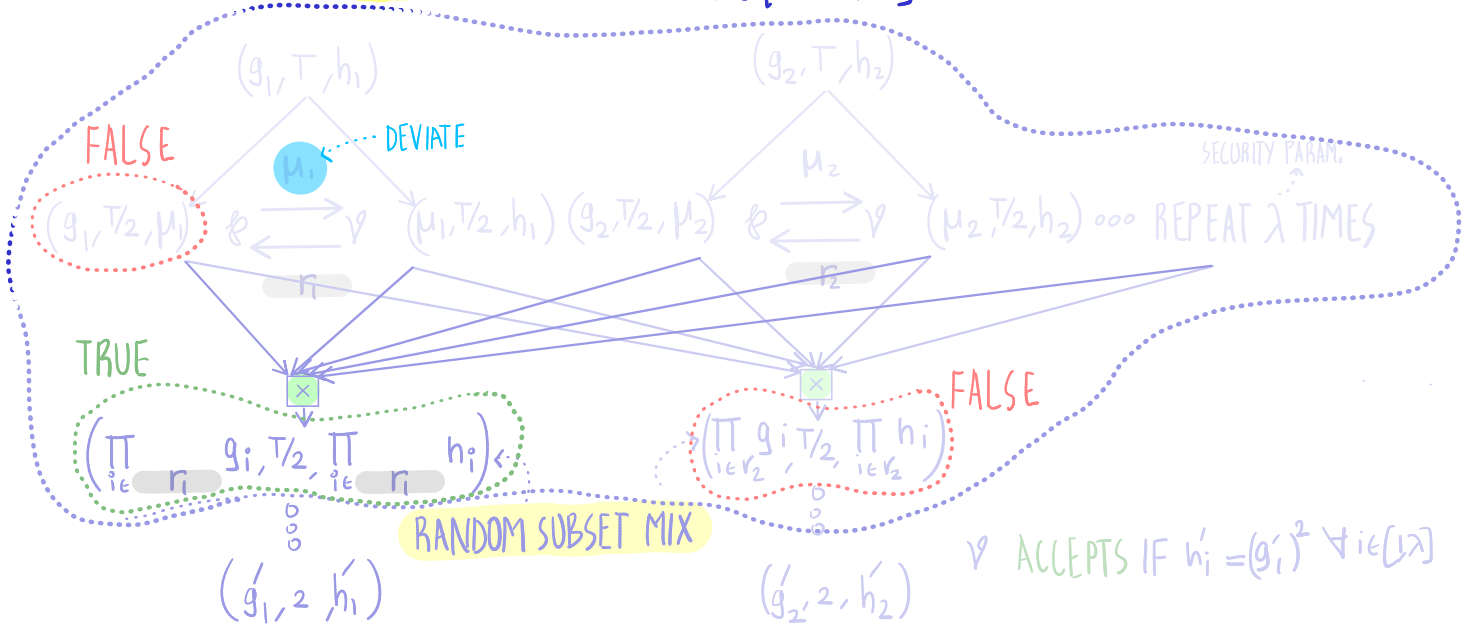
+ UNIQUE ?

SOUND ? ✓ ~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]



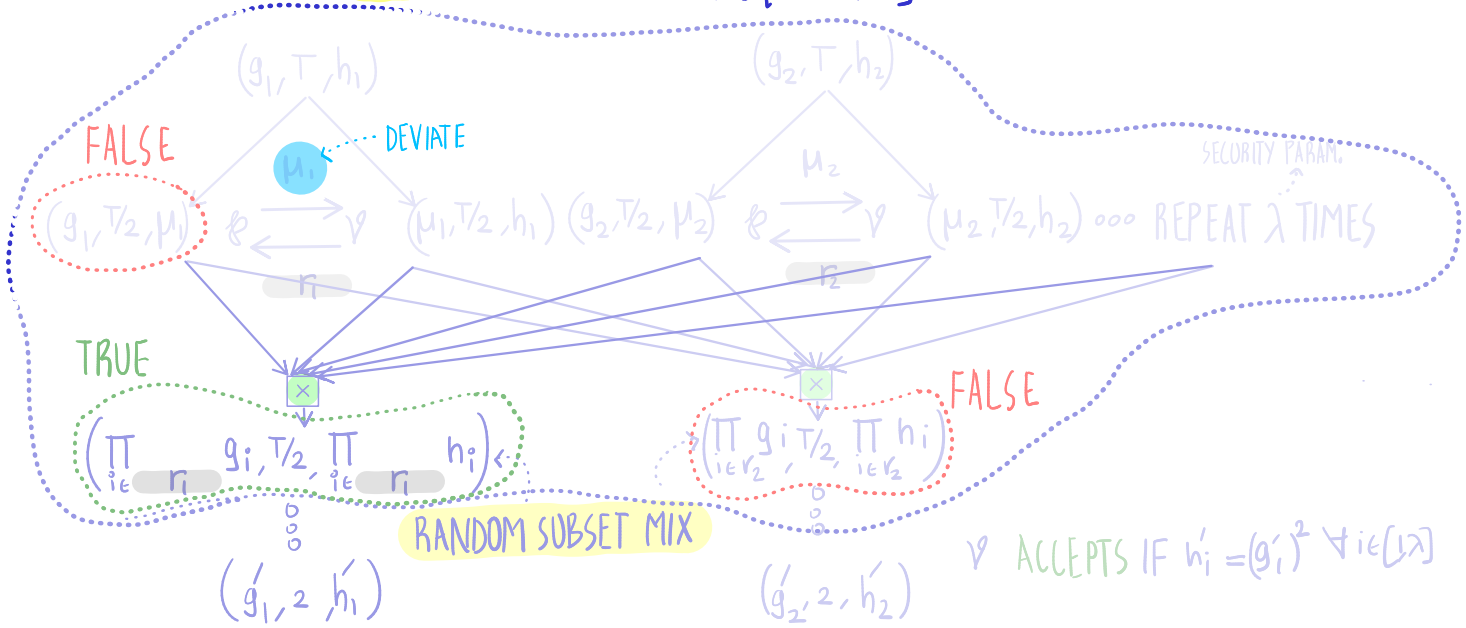
+UNIQUE? ✓ MIXING ⇒ DEVIATING LEADS TO $\mathcal{V}$ EVENTUALLY REJECTING

SOUND? ✓ ~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]



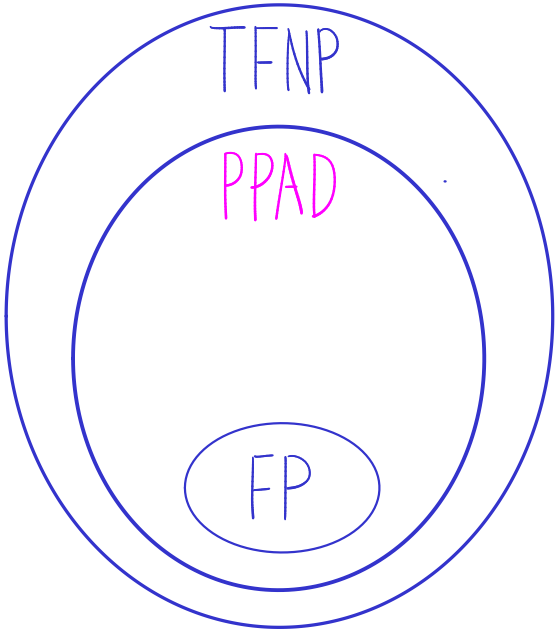
+UNIQUE? ✓ MIXING ⇒ DEVIATING LEADS TO $\mathcal{V}$ EVENTUALLY REJECTING

SOUND? ✓ ~PARALLEL AMPLIFICATION: SEE [BHRRS21]

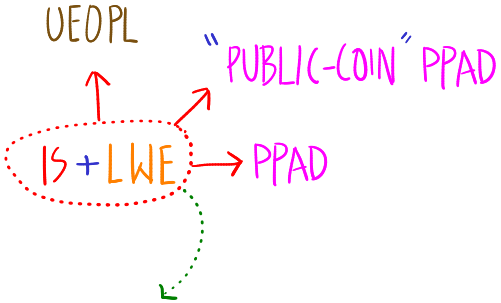
FIAT-SHAMIR? ✓ [HLR21] HASH FROM LWE

IN CONCLUSION...

IS + LWE → PPAD

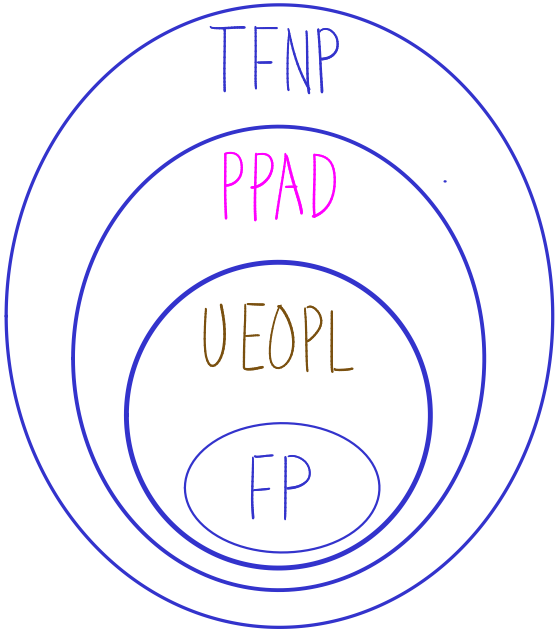


IN CONCLUSION...

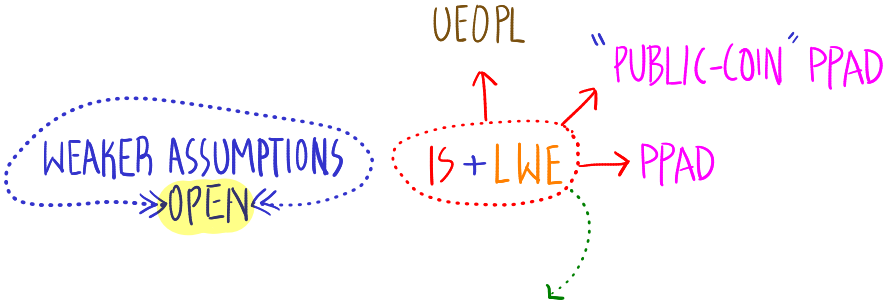


ABSTRACT BATCH-AND-OUTLINE PROTOCOL

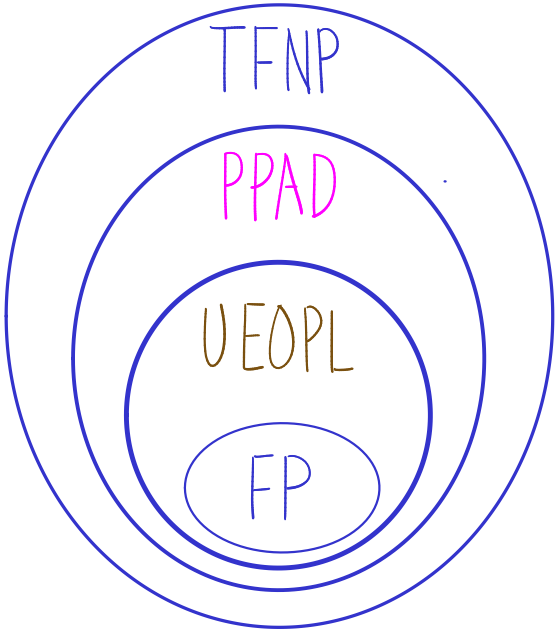
CAPTURES PREVIOUS WORKS: [CHKPRR19a/b, EFKP19, LV20, JKKZ21]



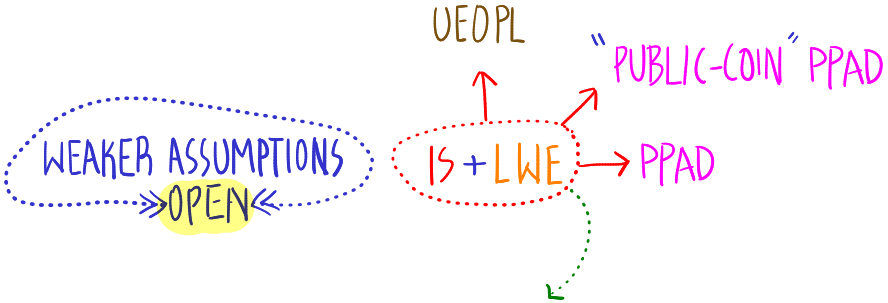
IN CONCLUSION...



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

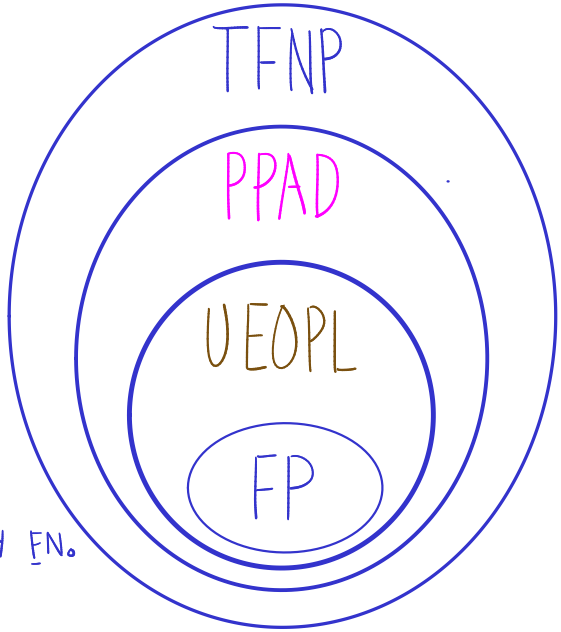


IN CONCLUSION...

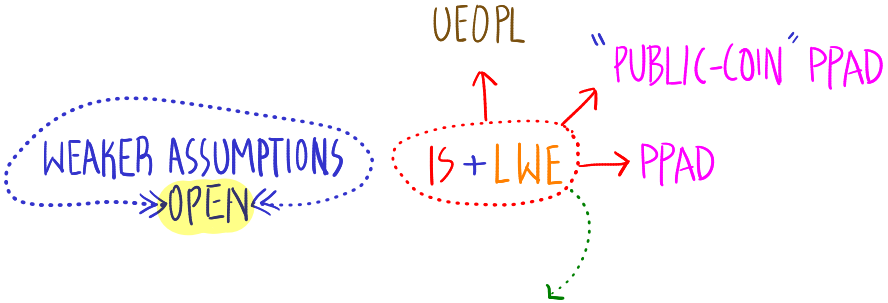


CAPTURES PREVIOUS WORKS: [CHKPRR19a/b, EFKP19, LV20, JKKZ21]

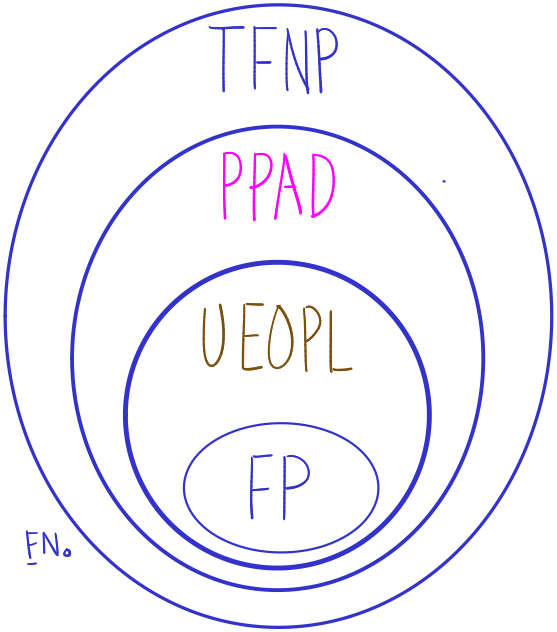
BONUS: SEQUENTIAL HARDNESS. IS+LWE ⇒ UNIQUE VDF ... VERIFIABLE DELAY FN.



IN CONCLUSION...



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



BONUS: SEQUENTIAL HARDNESS. IS+LWE ⇒ UNIQUE VDF. VERIFIABLE DELAY FN.

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

קרן עזריאלי
Azrieli Foundation

תוכנית עמיתי עזריאלי
Azrieli Fellows Program