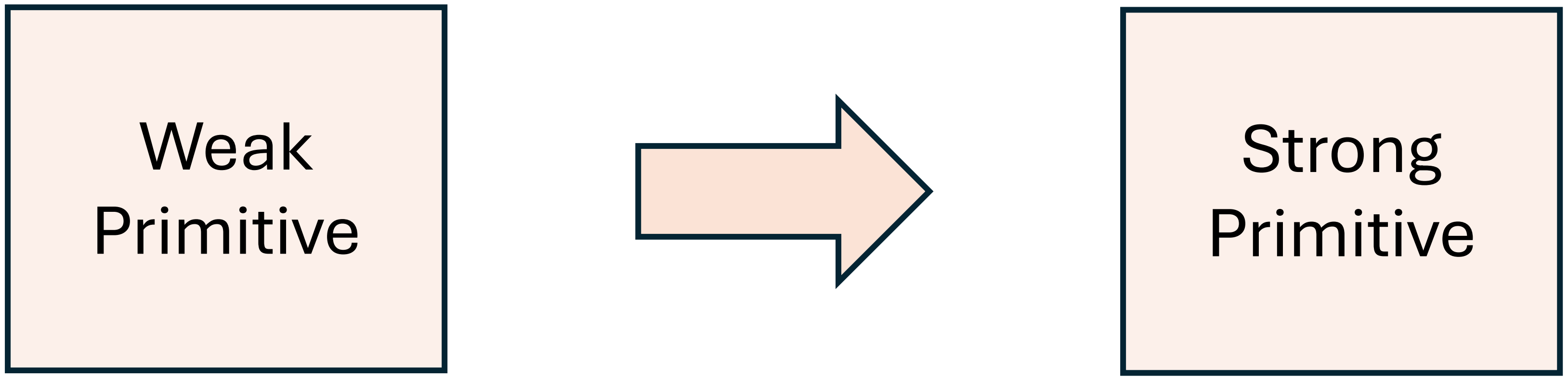
Amplification of Non-Interactive Zero Knowledge, Revisited

Nir Bitansky and Nathan Geier

New York University and Tel Aviv University

Security Amplification

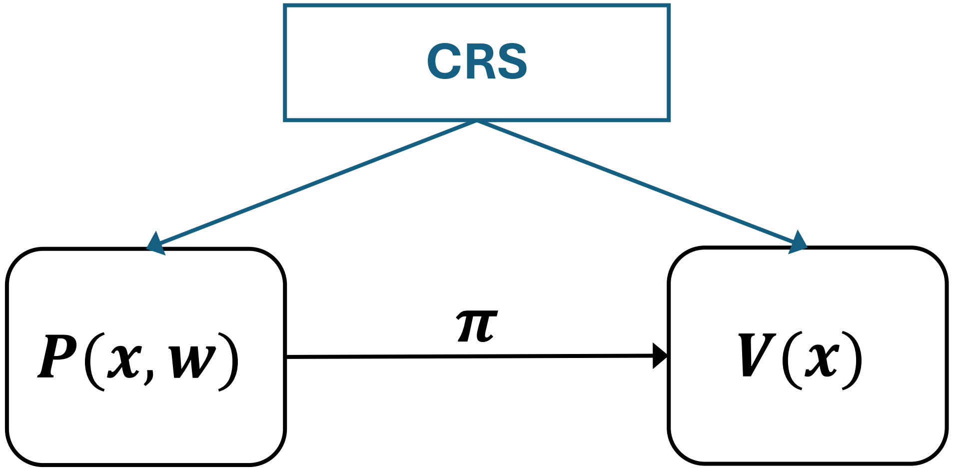


- Weak primitives are often easier to construct.
- Famous examples: Yao's OWF amplification and XOR lemma [Yao 82].

Non-Interactive Zero Knowledge

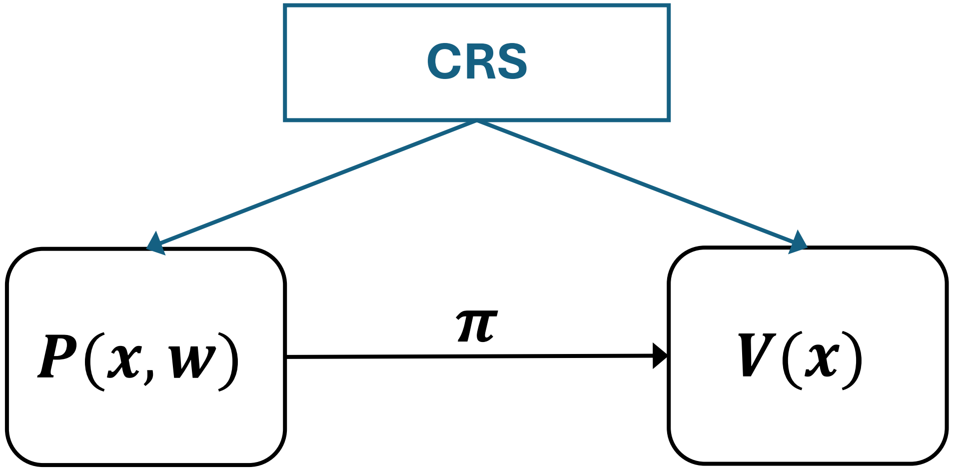
[Blum-Feldman-Micali 88]

- Completeness:
  $\forall (x, w) \in R_L \Rightarrow V$ accepts.
- Soundness:
  $\forall$malicious prover P^*
  $Pr[x \notin L \text{ and } V \text{ accepts}] = \text{negl.}$
- Zero Knowledge:
  $\exists$PPT SIM $\forall (x, w) \in R_L$
  $(crs, \pi) \approx \text{SIM}(x)$.



Weak NIZK

- Completeness:
  $\forall (x, w) \in R_L \Rightarrow V$ accepts.
- Soundness:
  $\forall$malicious prover P^*
  $Pr[x \notin L \text{ and } V \text{ accepts}] \leq \varepsilon_s$.
- Zero Knowledge:
  $\exists$PPT SIM $\forall (x, w) \in R_L$
  $(crs, \pi) \approx_{\varepsilon_z}$ SIM(x).



Weak NIZK — The Non-Trivial Case

- (1,0)-weak NIZK: prover sends nothing, verifier accepts.
- (0,1)-weak NIZK: prover sends witness in the clear.
- (p,1-p)-weak NIZK: p-biased bit in the CRS, indicating which of the above to run.
- Interested in the non-trivial case where $\varepsilon_s + \varepsilon_z < 1$.

Previous Results

Goyal, Jain and Sahai suggest a way to amplify weak NIZK for any constants $\varepsilon_s + \varepsilon_z < 1$.

- Based on MPC-in-the-head paradigm [Ishai-Kushilevitz-Ostrovsky-Sahai 07].
- Assuming sub-exponential PKE.
- Authors discovered a gap in their proof.

Our Results

- Amplifying NIZK **arguments** for NP assuming only **polynomially-secure** public-key encryption, for any constants $\varepsilon_s + \varepsilon_z < 1$.

Our Results

- Amplifying NIZK **arguments** for NP assuming only **polynomially-secure** public-key encryption, for any constants $\varepsilon_s + \varepsilon_z < 1$.
- Amplifying NIZK **proofs** for NP assuming only **one-way functions**, for any constants $\varepsilon_s + \varepsilon_z < 1$.

Our Results

- Amplifying NIZK **arguments** for NP assuming only **polynomially-secure** public-key encryption, for any constants $\varepsilon_s + \varepsilon_z < 1$.
- Amplifying NIZK **proofs** for NP assuming only **one-way functions**, for any constants $\varepsilon_s + \varepsilon_z < 1$.
- When the soundness error ε_s is negligible to begin with, we can also amplify NIZK arguments for NP assuming only one-way functions.

- Based on the hidden-bits paradigm [Feige-Lapidot-Shamir 99], reduction to pseudorandomness amplification.

Weak-NIZK Constructions?

- Currently unaware of weak NIZK from weaker assumptions, except weak NISZK from batch arguments [Bitansky-Kamath-Paneth-Rothblum-Vasudevan 24].
- Combiners: random choice is weak.
- We mostly view NIZK amplification as a foundational hardness amplification question.

Technical Overview

Outline

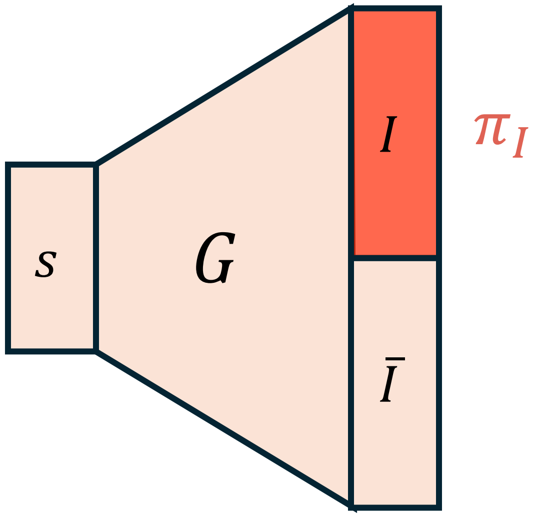
- Zero-Knowledge amplifier $\left(1-(1-\varepsilon_s)^k, \varepsilon_z^k\right)$.
- Soundness* amplifier $\left(\varepsilon_s^k, 1-(1-\varepsilon_z)^k\right)$.
- Combining the amplifiers.
- Proofs: soundness* for free.
- Arguments: soundness* from PKE.

Outline

- Zero-Knowledge amplifier $\left(1-(1-\varepsilon_s)^k, \varepsilon_z^k\right)$. ⇐ Main component
- Soundness* amplifier $\left(\varepsilon_s^k, 1-(1-\varepsilon_z)^k\right)$.
- Combining the amplifiers.
- Proofs: soundness* for free.
- Arguments: soundness* from PKE.

Hidden-Bits Generator

[Quach-Rothblum-Wichs 19, Kitagawa-Matsuda-Yamakawa 20]



- PRG $G: \{0,1\}^n \rightarrow \{0,1\}^{t(n)}$, with subset-consistency proofs.
- $G_{\bar{I}}, G_I, \pi_I \approx U, G_I, \pi_I$.
- Sufficient for NIZK (hidden-bits model [Feige-Lapidot-Shamir 99]).

HBG From Weak NIZK

- Prover generates $G(s_1), \dots, G(s_k)$ for PRG G and parameter k.
- Hidden bit-string is set to $\bigoplus_{i=1}^{k} G(s_i)$.
- Using weak NIZK, generate k independent consistency proofs $\pi_I(s_1), \dots, \pi_I(s_k)$ for the revealed $G_I(s_1), \dots, G_I(s_k)$.

HBG From Weak NIZK

- Prover generates $G(s_1), \ldots, G(s_k)$ for PRG G and parameter k.
- Hidden bit-string is set to $\bigoplus_{i=1}^{k} G(s_i)$.
- Using weak NIZK, generate k independent consistency proofs $\pi_I(s_1), \ldots, \pi_I(s_k)$ for the revealed $G_I(s_1), \ldots, G_I(s_k)$.

- Limited to $\varepsilon_z < 0.5$. What if last bit always leaked?

Tighter Amplification via Extraction

Maurer and Tessaro amplify weak PRGs using the concatenate and extract approach with a strong extractor:

$$\mathrm{Ext}(G(s_1), \dots, G(s_k); r), r \; .$$

Tighter Amplification via Extraction

Maurer and Tessaro amplify weak PRGs using the concatenate and extract approach with a strong extractor:

$$\mathrm{Ext}(G(s_1), \ldots, G(s_k); r), r \,.$$

- Issue: Ext_I may depend on all bits, not just G_I.

Tighter Amplification via Extraction

$\boldsymbol{E\left(F_{s_1}(1), \ldots, F_{s_k}(1)\right)}$	$\boldsymbol{E\left(F_{s_1}(2), \ldots, F_{s_k}(2)\right)}$	…	$\boldsymbol{E\left(F_{s_1}(t), \ldots, F_{s_k}(t)\right)}$
$F_{s_1}(1)$	$F_{s_1}(2)$	…	$F_{s_1}(t)$
$F_{s_2}(1)$	$F_{s_2}(2)$	…	$F_{s_2}(t)$
…	…	…	…
$F_{s_k}(1)$	$F_{s_k}(2)$	…	$F_{s_k}(t)$

- Use n-bit-output PRF F_s to generate t blocks, apply the extractor to each block separately.
- To reveal subset I, exhibit $F_{s_1}(I), \ldots, F_{s_k}(I)$, along with independent consistency proofs $\pi_I(s_1), \ldots, \pi_I(s_k)$.

Tighter Amplification via Extraction

	$\boldsymbol{E\left(F_{s_1}(1), \dots, F_{s_k}(1)\right)}$	$\boldsymbol{E\left(F_{s_1}(2), \dots, F_{s_k}(2)\right)}$	…	$\boldsymbol{E\left(F_{s_1}(t), \dots, F_{s_k}(t)\right)}$
$\boldsymbol{\pi_I(s_1)}$	$F_{s_1}(1)$	$F_{s_1}(2)$	…	$F_{s_1}(t)$
$\boldsymbol{\pi_I(s_2)}$	$F_{s_2}(1)$	$F_{s_2}(2)$	…	$F_{s_2}(t)$
…	…	…	…	…
$\boldsymbol{\pi_I(s_k)}$	$F_{s_k}(1)$	$F_{s_k}(2)$	…	$F_{s_k}(t)$

- Use n-bit-output PRF F_s to generate t blocks, apply the extractor to each block separately.
- To reveal subset I, exhibit $F_{s_1}(I), \dots, F_{s_k}(I)$, along with independent consistency proofs $\pi_I(s_1), \dots, \pi_I(s_k)$.

Open Questions

- Polynomially small gap: how to amplify $(0.5,\ 0.5 - 1/n)$?
- Zero-knowledge amplifier for non-adaptive soundness.
- Amplification for arguments without PKE.

Open Questions

- Polynomially small gap: how to amplify $(0.5,\ 0.5 - 1/n)$?
- Zero-knowledge amplifier for non-adaptive soundness.
- Amplification for arguments without PKE.

Thank you!

erc