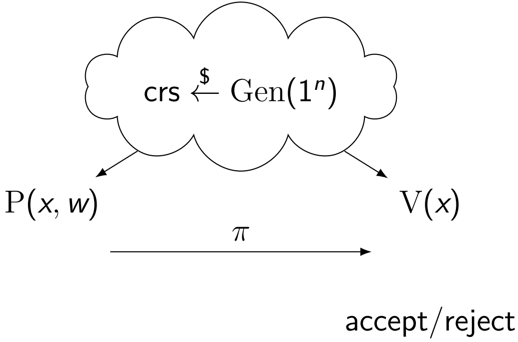
On Weak NIZKs, One-way Functions and Amplification

Suvradip Chakraborty (Visa Research)

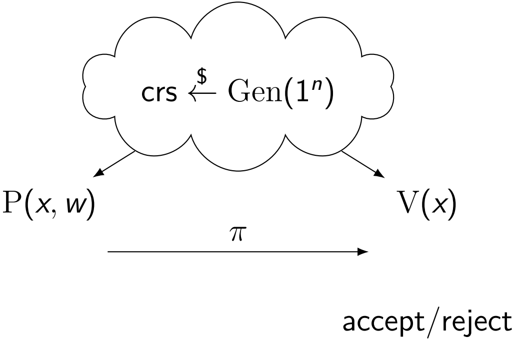
James Hulett (UIUC)

Dakshita Khurana (UIUC and NTT)

Non-Interactive Zero-Knowledge (for NP)

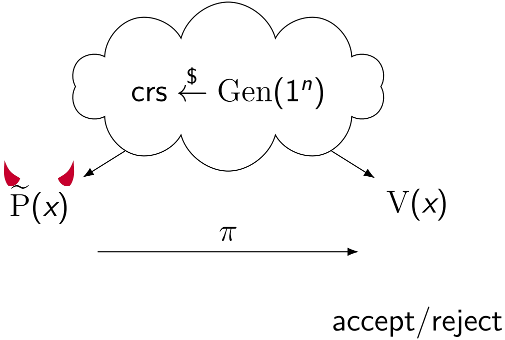


Non-Interactive Zero-Knowledge (for NP)



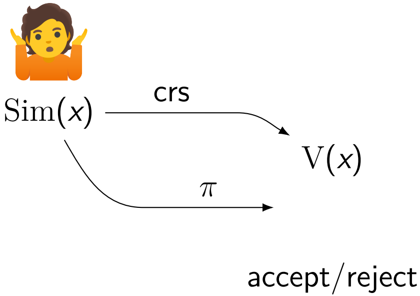
Completeness: If $x \in \mathcal{L}$, $\Pr[\mathrm{V}\text{ accepts}] \geq 1 - \epsilon_{\mathsf{c}}$.

Non-Interactive Zero-Knowledge (for NP)



Soundness: If $x \notin \mathcal{L}$, then for any nuPPT cheating prover $\widetilde{\mathrm{P}}$, $\Pr[\mathrm{V} \text{ accepts}] \leq \epsilon_{\mathsf{s}}$.

Non-Interactive Zero-Knowledge (for NP)



Zero-Knowledge: There is a simulator Sim that for every $x \in \mathcal{L}$ is ϵ_{zk} computationally indistiguishable from V's view.

NIZK and OWF

Key question: how “hard” are NIZKs to construct?
Do they *require* one-way functions?

NIZK and OWF

Key question: how “hard” are NIZKs to construct?
Do they *require* one-way functions?

[Ost91, OW93]: Yes*

NIZK and OWF

Key question: how "hard" are NIZKs to construct?
Do they *require* one-way functions?

[Ost91, OW93]: Yes*
*if ϵ_{c}, ϵ_{s}, and ϵ_{zk} are all negligible.

NIZK and OWF

Key question: how "hard" are NIZKs to construct?
Do they *require* one-way functions?

[Ost91, OW93]: Yes*
*if ϵ_{c}, ϵ_{s}, and ϵ_{zk} are all negligible.

Our goal: understand what happens if the error parameters are allowed to be large, even constant.

Why Weak NIZKs?

Why Weak NIZKs?

Recent work [GJS19,BKP+24,BG24,AK25] has shown that we can amplify "weak" NIZKs to get negligible errors.

- [BG24,AK25] only need one-way functions! (in some settings)

Why Weak NIZKs?

Recent work [GJS19,BKP+24,BG24,AK25] has shown that we can amplify "weak" NIZKs to get negligible errors.

- [BG24,AK25] only need one-way functions! (in some settings)

Viewpoint 1: understand if the hardness of constructing NIZKs is "inherent" or only comes from needing the errors to be small.

Why Weak NIZKs?

Recent work [GJS19,BKP+24,BG24,AK25] has shown that we can amplify "weak" NIZKs to get negligible errors.

- [BG24,AK25] only need one-way functions! (in some settings)

Viewpoint 1: understand if the hardness of constructing NIZKs is "inherent" or only comes from needing the errors to be small.

Viewpoint 2: if weak NIZKs give one-way functions, we can amplify "for free"!

Main Results

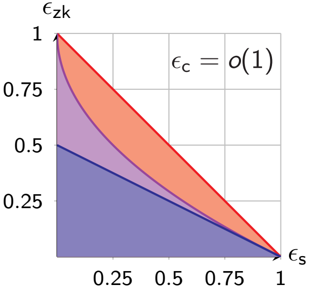
Suppose NP $\not\subseteq$ ioP/poly and we have a weak NIZK for NP. Then one-way functions exist if for any polynomial p, any of the following hold:

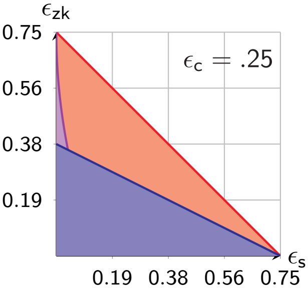
- $\epsilon_c(n) + \epsilon_s(n) + 2\epsilon_{zk}(n) < 1 - \frac{1}{p(n)}$
- $\epsilon_c(n) + \epsilon_{zk}(n) + 2\sqrt{\epsilon_s(n)} < 1 - \frac{1}{p(n)}$
- $\epsilon_c(n) = o(1)$, ϵ_s and ϵ_{zk} are constants, and $\epsilon_{zk} + \sqrt{\epsilon_s} < 1$

Main Results

Suppose NP $\not\subseteq$ ioP/poly and we have a weak NIZK for NP. Then one-way functions exist if for any polynomial p, any of the following hold:

- $\epsilon_c(n) + \epsilon_s(n) + 2\epsilon_{zk}(n) < 1 - \frac{1}{p(n)}$
- $\epsilon_c(n) + \epsilon_{zk}(n) + 2\sqrt{\epsilon_s(n)} < 1 - \frac{1}{p(n)}$
- $\epsilon_c(n) = o(1)$, ϵ_s and ϵ_{zk} are constants, and $\epsilon_{zk} + \sqrt{\epsilon_s} < 1$





Amplification Corollaries

Combining the third result with theorems from [BG24], we get "almost unconditional" amplification as a corollary.

Amplification Corollaries

Combining the third result with theorems from [BG24], we get “almost unconditional” amplification as a corollary.

We can* amplify a weak NIZK for NP to have negligible errors if:

- The weak NIZK has adaptive statistical soundness, with $\epsilon_{\mathsf{c}}(n)$ negligible, ϵ_{s} and ϵ_{zk} constants, and $\epsilon_{\mathsf{zk}} + \sqrt{\epsilon_{\mathsf{s}}} < 1$.
- The weak NIZK has adaptive computational soundness, with $\epsilon_{\mathsf{c}}(n)$ and $\epsilon_{\mathsf{s}}(n)$ negligible and ϵ_{zk} a constant less than 1.

Amplification Corollaries

Combining the third result with theorems from [BG24], we get "almost unconditional" amplification as a corollary.

We can* amplify a weak NIZK for NP to have negligible errors if:

- The weak NIZK has adaptive statistical soundness, with $\epsilon_{\mathsf{c}}(n)$ negligible, ϵ_{s} and ϵ_{zk} constants, and $\epsilon_{\mathsf{zk}} + \sqrt{\epsilon_{\mathsf{s}}} < 1$.
- The weak NIZK has adaptive computational soundness, with $\epsilon_{\mathsf{c}}(n)$ and $\epsilon_{\mathsf{s}}(n)$ negligible and ϵ_{zk} a constant less than 1.

(* as long as *either* NP $\not\subseteq$ ioP/poly or NP $\subseteq$ BPP)

Overview of Techniques

Each parameter regime uses different techniques to show that if one-way functions don't exist but NP has a weak NIZK, NP $\subseteq$ ioP/poly:

- $\epsilon_{\mathsf{c}}(n) + \epsilon_{\mathsf{s}}(n) + 2\epsilon_{\mathsf{zk}}(n) < 1 - \frac{1}{p(n)}$

- $\epsilon_{\mathsf{c}}(n) + \epsilon_{\mathsf{zk}}(n) + 2\sqrt{\epsilon_{\mathsf{s}}(n)} < 1 - \frac{1}{p(n)}$

- $\epsilon_{\mathsf{c}}(n) = o(1)$, ϵ_{s} and ϵ_{zk} are constants, and $\epsilon_{\mathsf{zk}} + \sqrt{\epsilon_{\mathsf{s}}} < 1$

Overview of Techniques

Each parameter regime uses different techniques to show that if one-way functions don't exist but NP has a weak NIZK, NP $\subseteq$ ioP/poly:

- $\epsilon_{\mathsf{c}}(n) + \epsilon_{\mathsf{s}}(n) + 2\epsilon_{\mathsf{zk}}(n) < 1 - \frac{1}{p(n)}$
  - Standard techniques from [OW93]: use Universal Extrapolation to sample a *simulated* proof relative to a *real* crs.
- $\epsilon_{\mathsf{c}}(n) + \epsilon_{\mathsf{zk}}(n) + 2\sqrt{\epsilon_{\mathsf{s}}(n)} < 1 - \frac{1}{p(n)}$
- $\epsilon_{\mathsf{c}}(n) = o(1)$, ϵ_{s} and ϵ_{zk} are constants, and $\epsilon_{\mathsf{zk}} + \sqrt{\epsilon_{\mathsf{s}}} < 1$

Overview of Techniques

Each parameter regime uses different techniques to show that if one-way functions don't exist but NP has a weak NIZK, NP $\subseteq$ ioP/poly:

- $\epsilon_c(n) + \epsilon_s(n) + 2\epsilon_{zk}(n) < 1 - \frac{1}{p(n)}$
  - Standard techniques from [OW93]: use Universal Extrapolation to sample a *simulated* proof relative to a *real* crs.
- $\epsilon_c(n) + \epsilon_{zk}(n) + 2\sqrt{\epsilon_s(n)} < 1 - \frac{1}{p(n)}$
  - Modify the above to reject any CRS that is "too much more likely to be simulated".
- $\epsilon_c(n) = o(1)$, ϵ_s and ϵ_{zk} are constants, and $\epsilon_{zk} + \sqrt{\epsilon_s} < 1$

Overview of Techniques

Each parameter regime uses different techniques to show that if one-way functions don't exist but NP has a weak NIZK, NP $\subseteq$ ioP/poly:

- $\epsilon_c(n) + \epsilon_s(n) + 2\epsilon_{zk}(n) < 1 - \frac{1}{p(n)}$
  - Standard techniques from [OW93]: use Universal Extrapolation to sample a *simulated* proof relative to a *real* crs.
- $\epsilon_c(n) + \epsilon_{zk}(n) + 2\sqrt{\epsilon_s(n)} < 1 - \frac{1}{p(n)}$
  - Modify the above to reject any CRS that is "too much more likely to be simulated".
- $\epsilon_c(n) = o(1)$, ϵ_s and ϵ_{zk} are constants, and $\epsilon_{zk} + \sqrt{\epsilon_s} < 1$
  - Parallel-repeat the weak NIZK a constant number of times until the new parameters satisfy the previous result.

Overview of Techniques

Each parameter regime uses different techniques to show that if one-way functions don't exist but NP has a weak NIZK, NP $\subseteq$ ioP/poly:

- $\epsilon_c(n) + \epsilon_s(n) + 2\epsilon_{zk}(n) < 1 - \frac{1}{p(n)}$
  - Standard techniques from [OW93]: use Universal Extrapolation to sample a *simulated* proof relative to a *real* crs.
- $\epsilon_c(n) + \epsilon_{zk}(n) + 2\sqrt{\epsilon_s(n)} < 1 - \frac{1}{p(n)}$
  - Modify the above to reject any CRS that is "too much more likely to be simulated".
- $\epsilon_c(n) = o(1)$, ϵ_s and ϵ_{zk} are constants, and $\epsilon_{zk} + \sqrt{\epsilon_s} < 1$
  - Parallel-repeat the weak NIZK a constant number of times until the new parameters satisfy the previous result.

CRS Checking

Our main technical insight is to modify the algorithm from [OW93] to:

- Estimate the probability that its CRS comes from Sim versus from Gen
- Reject immediately if the former is at least $\frac{1}{\sqrt{\epsilon_s}}$ times larger than the latter

CRS Checking

Our main technical insight is to modify the algorithm from [OW93] to:

- Estimate the probability that its CRS comes from Sim versus from Gen
- Reject immediately if the former is at least $\frac{1}{\sqrt{\epsilon_s}}$ times larger than the latter

This helps because one step in the [OW93] analysis involves changing *only* the CRS from real to simulated:

CRS Checking

Our main technical insight is to modify the algorithm from [OW93] to:

- Estimate the probability that its CRS comes from Sim versus from Gen
- Reject immediately if the former is at least $\frac{1}{\sqrt{\epsilon_s}}$ times larger than the latter

This helps because one step in the [OW93] analysis involves changing *only* the CRS from real to simulated:

- Any CRS that is “too likely simulated” contributes (almost) nothing to the probability the algorithm accepts $x \notin \mathcal{L}$
- Any other CRS can contribute *at most* $\frac{1}{\sqrt{\epsilon_s}}$ times as much to this probability in the simulated versus real case

CRS Checking

Our main technical insight is to modify the algorithm from [OW93] to:

- Estimate the probability that its CRS comes from Sim versus from Gen
- Reject immediately if the former is at least $\frac{1}{\sqrt{\epsilon_s}}$ times larger than the latter

This helps because one step in the [OW93] analysis involves changing *only* the CRS from real to simulated:

- Any CRS that is "too likely simulated" contributes (almost) nothing to the probability the algorithm accepts $x \notin \mathcal{L}$
- Any other CRS can contribute *at most* $\frac{1}{\sqrt{\epsilon_s}}$ times as much to this probability in the simulated versus real case

This replaces an *additive* ϵ_{zk} loss with a *multiplicative* $\frac{1}{\sqrt{\epsilon_s}}$ loss!

Future Directions

Future Directions

Can we get one-way functions from NIZKs with arbitrary (non-trivial) error parameters?

Generalization to interactive zero-knowledge?

Future Directions

Can we get one-way functions from NIZKs with arbitrary (non-trivial) error parameters?

Generalization to interactive zero-knowledge?

Improvements to amplification from one-way functions:

- Allow ϵ_{c} (and for arguments ϵ_{s}) to be non-negligible?
- Make uniformity preserving?

Future Directions

Can we get one-way functions from NIZKs with arbitrary (non-trivial) error parameters?

- Upcoming work: can work with any $\epsilon_c(n) + \epsilon_s(n) + \epsilon_{zk}(n) < 1 - \frac{1}{p(n)}$.

Generalization to interactive zero-knowledge?

Improvements to amplification from one-way functions:

- Allow ϵ_c (and for arguments ϵ_s) to be non-negligible?
- Make uniformity preserving?

Future Directions

Can we get one-way functions from NIZKs with arbitrary (non-trivial) error parameters?

- Upcoming work: can work with any $\epsilon_{\mathsf{c}}(n) + \epsilon_{\mathsf{s}}(n) + \epsilon_{\mathsf{zk}}(n) < 1 - \frac{1}{p(n)}$.

Generalization to interactive zero-knowledge?

- Upcoming work: some progress, but seems stuck at constant rounds.

Improvements to amplification from one-way functions:

- Allow ϵ_{c} (and for arguments ϵ_{s}) to be non-negligible?
- Make uniformity preserving?

Thanks!