Strong Batching for Non-Interactive Statistical Zero-Knowledge by Preserving Entropy under Hash Composition.

Changrui Mu [1]

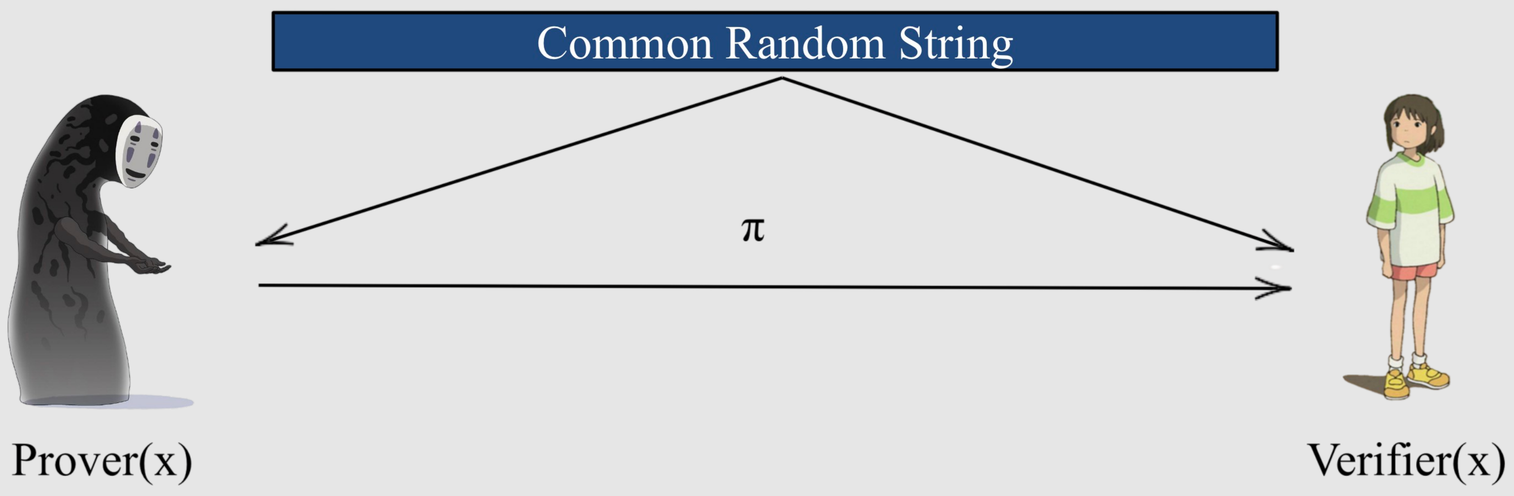
supervisor: Prashant Nalini Vasudevan [1]

[1]National University of Singapore

This poster is based on the"Strong Batching for Non-Interactive Statistical Zero-Knowledge" [Mu, Nassar, Rothblum, and Vasudevan; Eurocrypt2024].

Scan for handouts!

Non-Interactive Statistical Zero Knowledge Proofs [GMR89; BFM88].



1. Completeness: If $x \in$ YES: Verifier accept with 99%.
2. Soundness: If $x \in$ NO: No Prover can make Verifier accept with probability more than $\frac{1}{3}$.
3. Statistical Zero-Knowledge:
   There exists some efficient simulator algorithm Sim such that on any YES input $x \in$ YES, it can simulate a distribution *statistically* close to the Verifier's view in the protocol:

$$\text{Sim}(x) \approx_s CRS||\pi.$$

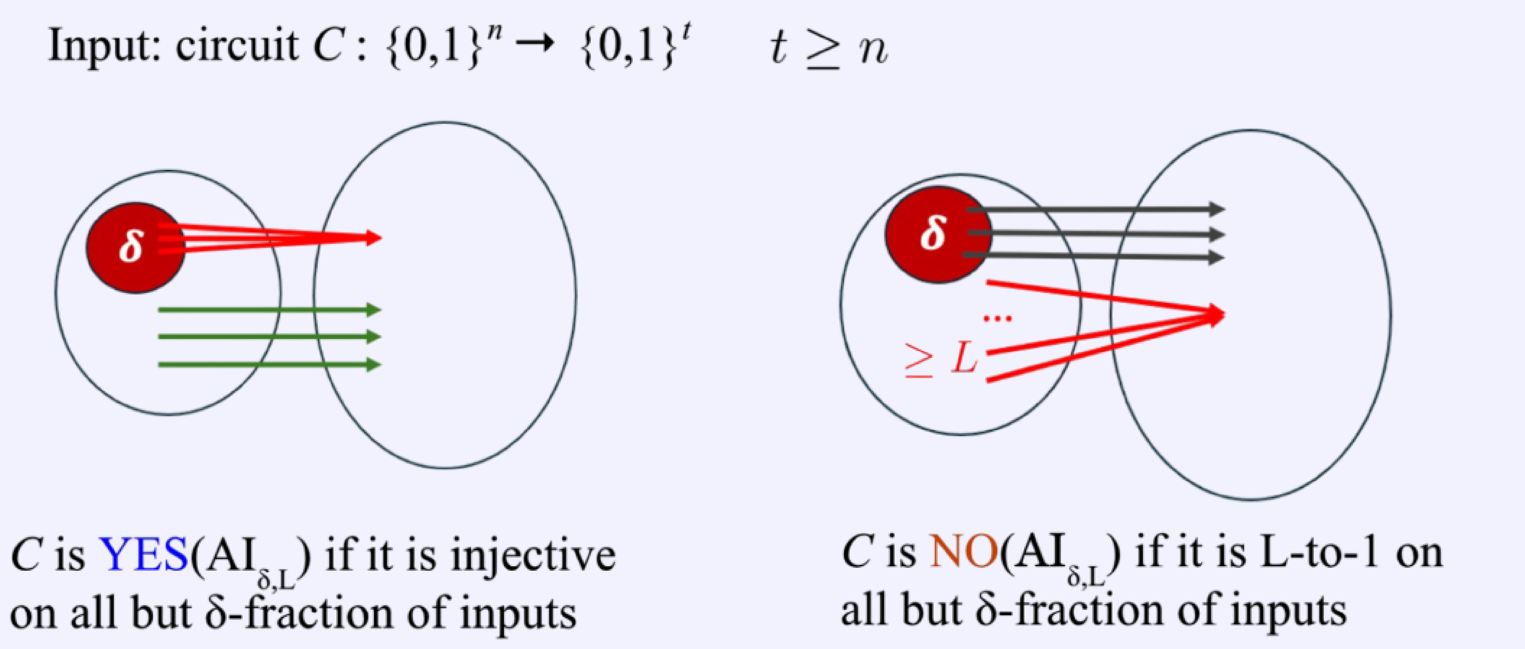
We call the class of problems that have non-interactive statistical zero-knowledge proofs **NISZK** problems.

NISZK Complete Problems [SCPY98; GSV99]

The class NISZK has complete problems. That is, there exists a problem Π such that:

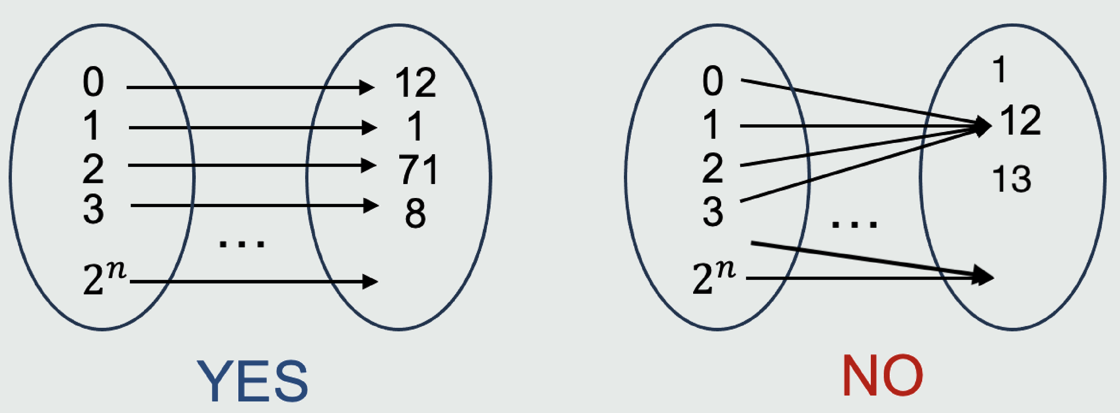
- Π can be proved in non-interactive statistical zero-knowledge proof.
- Every promise problem that has non-interactive statistical zero-knowledge proof can be reduced to Π.

Theorem 1: Approximate Injectivity (AI) [KRRSV20; KRV21]

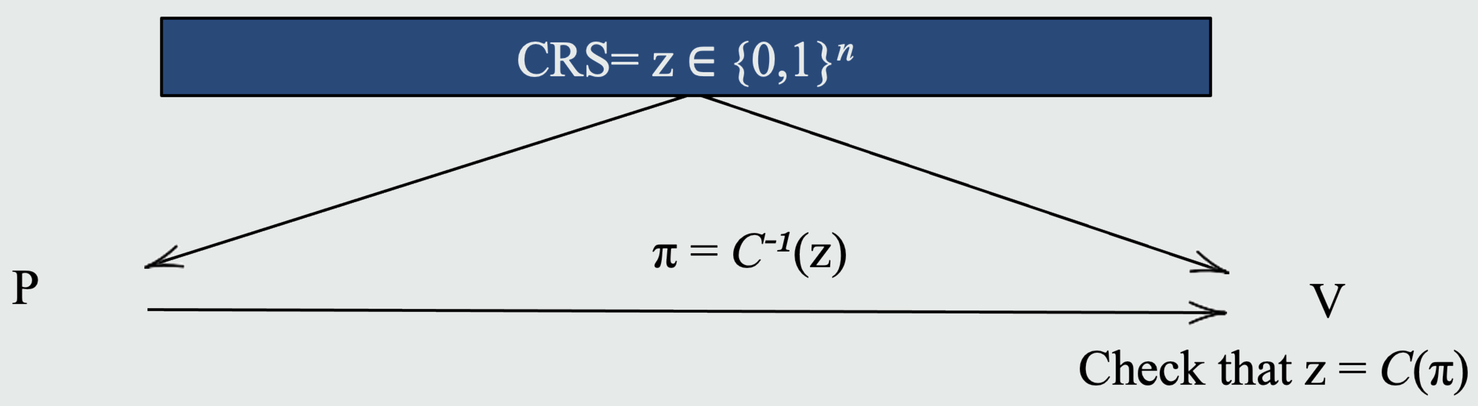


$\mathbf{AI}_{\delta,\mathbf{L}}$ *is* ***NISZK-complete*** *for* $\mathbf{L(n)} < \mathbf{2^{n^{0.1}}}, \delta > \mathbf{2^{-n^{0.1}}}$*.[KRRSV20; KRV21]*

How is Injectivity related to Non-Interactive Statistical Zero-Knowledge?



- Input: length-preserving circuit $C : \{0,1\}^n \to \{0,1\}^n$



- Completeness: Perfect, because any value of z has a preimage of the permutation.
- Soundness: NO case, the circuit is L-to-one, a random z doesn't have a preimage with probability at least 1-1/L.
- ZK: simulator samples x and output $(crs = C(x), \pi = x)$. Perfect Zero-Knowledge

NISZK Batching [KRRSV20; KRV21; MNRV24]

In batching verification setting, there are k instances to verify, we want to verify them in SZK proof with communication better than naive repetition. Specifically, if m is the number of communication bits required for one instance, we want the communication cost for verifying k instances to be much less than $k \cdot m$.

	Communication Complexity	Round Complexity	Interaction
[KRRSV20; KRV21]	$O(poly(m) + k)$	k	Interactive
This Work	$poly(m, \log k)$	1	Non-interactive

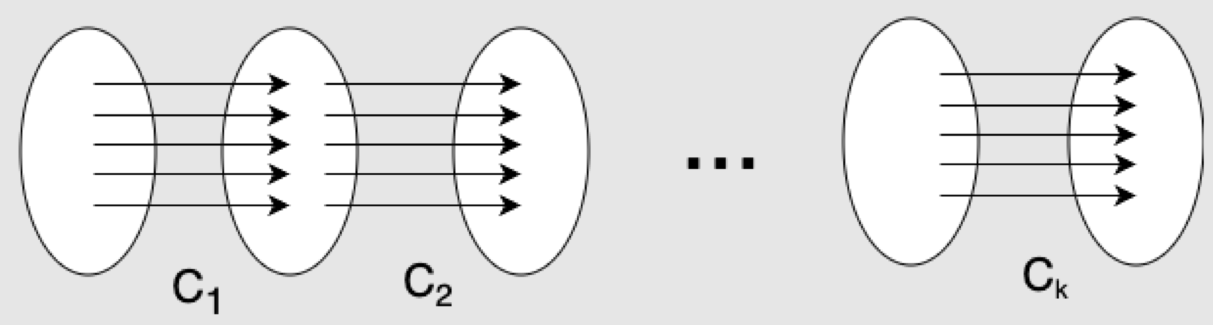
Theorem 2: NISZK Strong Batching [MNRV24]

Suppose a problem Π has NISZK protocol with $m(n)$ bits of communication and CRS length, then for any $k \in O(2^{n^{0.01}})$, there exists a NISZK protocol that proves k instances $x_1, x_2, \ldots, x_k$ with $poly(m, \log k)$ communication and CRS length.

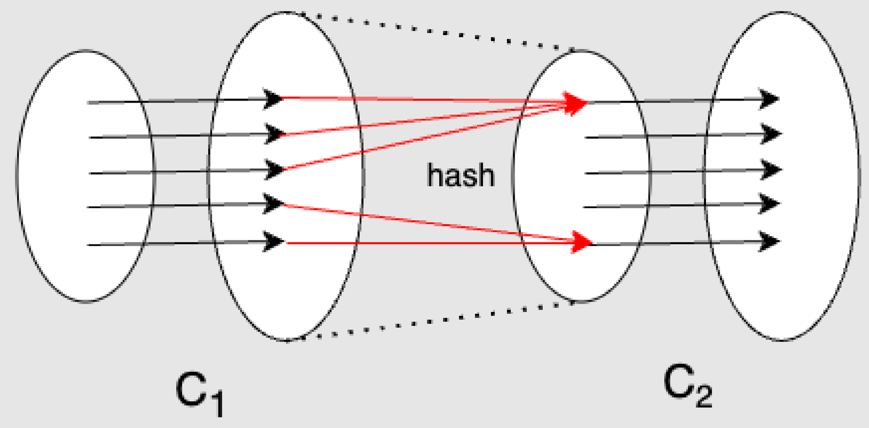
Reduce k instances to one

If k circuits are length preserving, direct composition gives a new length-preserving instance:

$$\bar{C} = C_k \circ \cdots \circ C_1$$

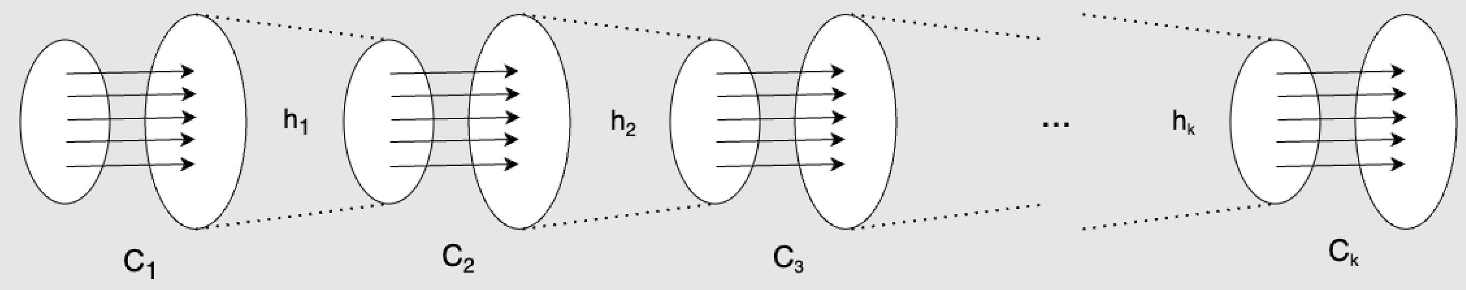


When $t > n$, we can not compose directly, and using random hash functions to connect them is a natural idea. However, even one round of such composition on injective circuits will introduce massive collisions.



We observe and prove that the collision probability is preserved under the hash composition

$$\bar{C} = h_k \circ C_k \circ \cdots \circ h_1 \circ C_1.$$



Specifically:

- If $C_1, \ldots, C_k \in$ YES, with 1-negl probability: $cp(\bar{C}) = \Pr_{x_1,x_2 \leftarrow \{0,1\}^n}[\bar{C}(x_1) = \bar{C}(x_2)] \leq \frac{2k+1}{2^n}$ or, the Rényi Entropy (order 2) is big:

$$H_2(\bar{C}) = -\log cp(\bar{C}) \geq n - \log k + 1.$$

- If some $C_i \in$ NO, the Max Entropy of $\bar{C}$ is small:

$$H_0(\bar{C}) = \log |support(\bar{C})| \leq n - \log L,\ L \in O(2^{n^{0.01}}).$$

Reduce Entropy to Uniformity/Injectivity

Input	Yes/No		Problem Name	Completeness
$C_1,\ldots,C_k$	All Injective	Exists L-to-1	Approximate Injectivity	**NISZK-Complete** [KRRSV]
$\bar{C}_k=(h_k \cdot C_k \cdot \ldots \cdot h_1 \cdot C_1)$	High Smooth Rényi Entropy	Low Max Entropy	Smooth Entropy Approx	**NISZK-Complete** (This work)
$\hat{C}$=h, h($\bar{C}_k$)	Close to uniform	Far from uniform	Statistically Close to Uniformity	**NISZK-Complete** [GSV]
$\hat{C}(x_1),\ldots,\hat{C}(x_k)$, g, g($x_1,\ldots, x_k$)	Injective	L-to-1	Approximate Injectivity	**NISZK-Complete** [KRRSV]

Asymptotic Equipartition Property + Load balancing

Leftover Hash Lemma

The prover and verifier will reduce k instances of a NISZK-complete problem to one instance, and run one execution of NISZK protocol on the single instance. Note that the communication cost of the protocol is dependent on the input/output length of the circuit, and thus will not increase much.

What's More

- Derandomization: The Collision Probability of the Composited Circuit can be modelled by a Read-Once Branching Program. Nisan's pseudorandom generator[Nis92] is used to sample hash functions, which derandomizes the Common Random String (CRS).
- [KRV24]: **Doubly-Efficient** Batch Verification in SZK for **NISZK** $\cap$ **UP**.

References

- O. Keret, R. D. Rothblum, and P. N. Vasudevan. *Doubly-Efficient Batch Verification in Statistical Zero-Knowledge*. Cryptology ePrint Archive, Paper 2024/781. https://eprint.iacr.org/2024/781. 2024. URL: https://eprint.iacr.org/2024/781.
- C. Mu, S. Nassar, R. D. Rothblum, and P. N. Vasudevan. "Strong Batching for Non-Interactive Statistical Zero-Knowledge". In: *IACR Cryptol. ePrint Arch.* (2024). https://eprint.iacr.org/2024/229. URL: https://eprint.iacr.org/2024/229.
- I. Kaslasi, R. D. Rothblum, and P. N. Vasudevan. "Public-Coin Statistical Zero-Knowledge Batch Verification Against Malicious Verifiers". In: *Advances in Cryptology - EUROCRYPT 2021 - 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Vol. 12698. Lecture Notes in Computer Science. Springer, 2021, pp. 219–246. DOI: 10.1007/978-3-030-77883-5_8.
- I. Kaslasi, G. N. Rothblum, R. D. Rothblum, A. Sealfon, and P. N. Vasudevan. "Batch Verification for Statistical Zero Knowledge Proofs". In: *Theory of Cryptography - 18th International Conference, TCC 2020*. Vol. 12551. Lecture Notes in Computer Science. Springer, 2020, pp. 139–167. DOI: 10.1007/978-3-030-64378-2_6.
- O. Goldreich, A. Sahai, and S. Vadhan. "Can Statistical Zero Knowledge Be Made Non-interactive? or On the Relationship of SZK and NISZK". In: *Advances in Cryptology — CRYPTO' 99*. Berlin, Heidelberg: Springer Berlin Heidelberg, 1999, pp. 467–484. ISBN: 978-3-540-48405-9.
- A. D. Santis, G. D. Crescenzo, G. Persiano, and M. Yung. "Image Density is Complete for Non-Interactive-SZK (Extended Abstract)". In: *Automata, Languages and Programming, 25th International Colloquium, ICALP'98, Proceedings*. Vol. 1443. Lecture Notes in Computer Science. Springer, 1998, pp. 784–795. DOI: 10.1007/BFb0055102.
- N. Nisan. "Pseudorandom generators for space-bounded computation". In: *Comb.* 12.4 (1992), pp. 449–461. DOI: 10.1007/BF01305237.
- S. Goldwasser, S. Micali, and C. Rackoff. "The Knowledge Complexity of Interactive Proof Systems". In: *SIAM J. Comput.* 18.1 (1989), pp. 186–208. DOI: 10.1137/0218012.
- M. Blum, P. Feldman, and S. Micali. "Non-Interactive Zero-Knowledge and Its Applications (Extended Abstract)". In: *Proceedings of the 20th Annual ACM Symposium on Theory of Computing*. ACM, 1988, pp. 103–112. DOI: 10.1145/62212.62222.