CONJURA · OPEN PROBLEM

Batch Verification for Statistical Zero Knowledge

Done non-interactively; the interactive class is the "most pressing open question"

Status. Statement: AI-written from Changrui Mu, Shafik Nassar, Ron D. Rothblum and Prashant Nalini Vasudevan, *Strong Batching for Non-Interactive Statistical Zero-Knowledge*, IACR ePrint 2024/229. Not yet checked by a human. Their Theorem 1.1 gives a batch NISZK proof with communication $\mathrm{poly}(n, \log k)$ for k instances; they name the SZK analogue as "[t]he most pressing open question" in their discussion. A $\mathrm{poly}(n)$ dependence is unavoidable even at $k = 1$, so $\log k$ is the right target in the second parameter.

Category. *Zero Knowledge.*

Conjecture (informal). *Proving k statements should cost less than proving each one separately. For zero-knowledge proofs this is delicate, because the obvious savings — reuse randomness, combine instances — are exactly the moves that threaten the zero-knowledge property. For the non-interactive class* NISZK *the source settles it: k instances can be batched into a single proof whose communication grows only logarithmically in k. For the interactive class* SZK*, which is larger and where the analogous protocols are the older and better studied ones, nobody knows. The source calls it the most pressing question its work leaves.*

1 The setting

Write $\Pi^{\otimes k}$ for the set of k-tuples of equal-length instances all of which belong to Π. Batch verification asks for a proof for $\Pi^{\otimes k}$ substantially cheaper than k independent executions, while preserving the proof system's guarantees — here, statistical zero knowledge.

What the source proves is the non-interactive case, in a strong form.

Theorem 1 (Batch proofs for NISZK, [MNRV24, Theorem 1.1]).

Suppose $\Pi \in \mathsf{NISZK}$ *and* $k = k(n) \in \mathbb{N}$ *with* $k(n) \leq 2^{n^{0.01}}$*, where* n *is the length of a single instance of* Π*. Then* $\Pi^{\otimes k}$ *has an* NISZK *protocol in which the communication complexity and the length of the common random string are* $\mathrm{poly}(n, \log k)$*. The completeness, soundness and zero-knowledge errors are all negligible in* n *and* k*, and the verifier runs in time* $\mathrm{poly}(n, k)$.

Two things about the shape of that bound. The source records that "a $\mathrm{poly}(n)$ dependence in the communication complexity is inevitable, even when $k = 1$, assuming the existence of a sub-exponentially hard problem in NISZK", which follows from known limitations on laconic provers. So $\mathrm{poly}(n)$ is not slack, and $\log k$ is the aggressive part. And the protocol is obtained by reducing to NISZK-complete problems, which matters for Remark 4.

2 Notation and parameters

- n is the length of a single instance; $k = k(n)$ the number of instances batched.
- $\Pi^{\otimes k}$ is the k-fold conjunction: tuples all of whose components are in Π.
- SZK is the class with statistical zero-knowledge *interactive* proofs; NISZK its non-interactive counterpart, with a common random string. $\mathsf{NISZK} \subseteq \mathsf{SZK}$.
- The target is total communication; the source's NISZK result also bounds the common random string.

3 The conjecture

Conjecture 1 ([MNRV24, §1.3, item 1]). *For every* $\Pi \in \mathsf{SZK}$ *there exists an* SZK *proof for* $\Pi^{\otimes k}$ *with communication* $\mathrm{poly}(n, \log k)$.

Remark 1 (How the source states it, and the weaker fallback it offers). Page 12: "The most pressing open question is whether a similar result holds for SZK – namely, for every $\Pi \in \mathsf{SZK}$ does there exist an SZK proof for $\Pi^{\otimes k}$ with communication $\mathrm{poly}(n, \log k)$? Or, alternatively, one that features less strigent, yet non-trivial, communication such as sub-linear dependence on k?"

Two targets, and the second is much weaker: *any* sub-linear dependence on k would already be non-trivial. A resolution should say which it achieves. Conjecture 1 records the strong form because that is the one the source names first and the one matching what it proved for NISZK; a sub-linear-in-k result is genuine progress and should be reported as partial rather than as a settlement.

Remark 2 (Why the non-interactive proof does not obviously transfer). The source's route is specific and its steps are what a SZK argument would have to replace. It reduces the k instances to k instances of an NISZK-complete problem, then reduces those to a single instance of another complete problem, using two technical observations: that hash functions with bounded independence — 4-wise suffices — preserve very specific types of entropies, and that a cascade of such hash functions can be derandomized while still preserving that behaviour.

Both steps lean on the structure of the NISZK-complete problems, which are entropy-approximation problems. SZK has its own complete problems (statistical difference), and whether the same entropy-preserving and derandomization machinery applies to them is precisely what is not known.

Remark 3 (What is known on the interactive side already). This is not a question with no prior work: the source positions itself against a line including Kaslasi et al. and Kaslasi, Rothblum and Vasudevan on batch verification, and notes neighbouring results on zero-knowledge proofs for conjunctions and on computationally sound protocols for monotone policies within NP. What is absent is a $\mathrm{poly}(n, \log k)$ bound for all of SZK.

Remark 4 (Neighbouring questions in the same list, none of them this one). The source lists two more. First, on *prover efficiency*: problems in $\mathsf{SZK} \cap \mathsf{NP}$ have SZK protocols with an efficient prover given an NP-witness, but all current batch protocols proceed by reducing to complete problems and so do not preserve that efficiency; is there a batch protocol even for $\mathsf{NISZK} \cap \mathsf{NP}$ that does? Second, on *rate*: can the multiplicative overhead be a fixed constant, i.e. communication $O(c) + \mathrm{polylog}(n, k)$ where c is the communication for a single instance, and can that constant be pushed toward 1? The source notes this "might necessitate avoiding the complete problems, since the reduction introduces a polynomial overhead".

Both are consequences of the same reduction-to-complete-problems route as Remark 2, which is why that route is the thing to attack.

Remark 5 (Bounds on k are part of the statement). Theorem 1 carries the hypothesis $k(n) \leq 2^{n^{0.01}}$. Conjecture 1 as the source phrases it names no range for k; a resolution should state the range it covers, since a result for k polynomial in n is weaker than one matching the NISZK theorem's reach.

4 Bibliography

[MNRV24] Changrui Mu, Shafik Nassar, Ron D. Rothblum and Prashant Nalini Vasudevan. *Strong batching for non-interactive statistical zero-knowledge.* IACR ePrint 2024/229. The source. Theorem 1.1 is on page 4 and re-proved on page 20; the discussion and open problems are Section 1.3 on page 12.

[GVW02] Oded Goldreich, Salil Vadhan and Avi Wigderson. *On interactive proofs with a laconic prover.* Computational Complexity, 2002. One of the two works the source cites for the inevitability of a poly(n) dependence even at $k = 1$.

[GH98] Oded Goldreich and Johan Håstad. *On the complexity of interactive proofs with bounded communication.* Information Processing Letters, 1998. The other.

[NV06] Minh-Huyen Nguyen and Salil Vadhan. *Zero knowledge with efficient provers.* STOC 2006. The result that problems in SZK ∩ NP have SZK protocols with an efficient prover, which the source's prover-efficiency question is measured against. [UNVERIFIED] — cited in the source as [NV06]; the bibliographic detail here is inferred.

[KRR+20] Inbar Kaslasi, Guy N. Rothblum, Ron D. Rothblum, Adam Sealfon and Prashant Nalini Vasudevan. *Batch verification for statistical zero knowledge proofs.* TCC 2020. The prior batch-verification protocols the source simplifies and strengthens. [UNVERIFIED] — cited in the source as [KRR+ 20]; the bibliographic detail here is inferred.