CONJURA · OPEN PROBLEM

A Designated-Verifier SNARG with One Group Element and $\tau + o(\tau)$ Bits

Generic group model, soundness error $2^{-\tau+\log\log\lambda}$, linear CRS

Status. Statement: AI-written from Gal Arnon, Jesko Dujmovic and Yuval Ishai, *Designated-Verifier SNARGs with One Group Element*, IACR ePrint 2025/517. Not yet checked by a human. Numbered Conjecture 1.3 of the source. Its own theorems achieve one group element plus $O(\tau)$ bits, and (with a random oracle) one group element, one hash output and about 2τ bits; the conjecture halves the additive term to $\tau + o(\tau)$ and asks for no random oracle.

Category. *Proof Systems.*

Conjecture (informal). *A designated-verifier SNARG lets a prover convince one particular verifier, who holds a secret verification state, that a circuit is satisfiable — with a proof far shorter than the witness. In the generic group model the source brings the proof down to a single group element plus a number of extra bits proportional to the desired soundness level τ, and with the help of a random oracle down to one group element, one hash output and about 2τ bits:* 695 *bits for 2^{-80} soundness at a* 128*-bit security level, roughly half the best pairing-based SNARG. Two of the sources of slack in that count are identified but not removed: the analysis of how malleable its packed ElGamal encryption really is, and the fact that the linear PCPs it uses spend two bits of answer per bit of soundness. Fix both and the additive term should fall to $\tau + o(\tau)$ — about* 340 *bits in the same concrete setting. That is the source's Conjecture 1.3, and nothing in the paper establishes it.*

1 The setting

Barta, Ishai, Ostrovsky and Wu [BIOW20] constructed designated-verifier SNARGs in the generic group model whose proof is two group elements, but only with inverse-polynomial soundness; for negligible soundness every previous construction needed a super-

constant number of group elements. The source closes that gap. Its Theorem 1.1 gives a dv-SNARG for Boolean circuit satisfiability with soundness error $2^{-\tau} + O(t^2 2^{-\lambda})$ against t-query adversaries, proof size one $\mathbb{G}$-element plus $O(\tau)$ additional bits, and CRS size $O(\tau s)$ group elements; its Theorem 1.2, additionally using a random oracle for collision resistance, reduces the additive term to $\lceil 2\tau \log p/(\log p - \Theta(1))\rceil$ bits at the cost of one extra hash output and a CRS of $O(\tau s \cdot \mathrm{poly}(p))$ elements.

Both come from extending the compiler of Bitansky et al. [BCI+13] — linear-only encryption plus a linear PCP — to *compressible* encryption schemes, instantiated with packed ElGamal. The bookkeeping that decides the proof size is how much malleability a generic-group adversary has against packed ElGamal, and the source says plainly that its bound there is loose: "we believe that our analysis is quite loose, and conjecture that an even a slightly simpler construction can achieve a better level of soundness."

The second slack is in the linear PCP. The source's construction is insensitive to the number of queries but sensitive to the ratio μ between the total bit-length of the LPCP answers and the soundness level τ; the LPCPs it uses have $\mu \approx 2$, which is exactly the 2τ additive term. LPCPs with $\mu \approx 1$ are known to follow from hardness-of-approximation results for MAXLIN [Has01], but they have non-negligible completeness error and, the source judges, "seem practically infeasible"; the route through amortised-query-complexity PCPs and universal factor graphs looks practically infeasible too. The source leaves designing practical LPCPs with $\mu \approx 1$ open.

Conjecture 1.3 of the source is what both fixes together would buy. It is stated as a numbered conjecture, it is not proved anywhere in the paper, and the parameters below are its own.

2 Notation and parameters

- λ is the security parameter; $\mathbb{G} = \mathbb{G}_\lambda$ is a generic group of order about 2^λ whose elements are described by λ bits.
- τ is the soundness parameter, t the number of generic-group oracle queries an adversary makes, s the size of the Boolean circuit whose satisfiability is proved.
- $R = \{(x, w)\}$ is the relation; $L(R)$ its language.
- Proof size is measured as a number of $\mathbb{G}$-elements plus a num-

ber of additional bits; CRS size as a number of $\mathbb{G}$-elements.

3 The conjecture

Definition 1 (Generic group model, Shoup's version, [ADI25, Definition 3.2]). For a prime p', the oracle holds a permutation f from the label space L — binary representations of $0,\ldots,p'-1$ — to the group $(\mathbb{Z}_{p'},+)$, sampled uniformly at the start of the security game, and all parties are given the label $g \leftarrow f^{-1}(1)$. The oracle G takes two labels χ_1,χ_2 and returns $f^{-1}(f(\chi_1)+f(\chi_2))$. We write $G \leftarrow \mathsf{GGM}(\lambda)$ for sampling such an oracle of size at least 2^λ.

Definition 2 (dv-SNARG in the generic group model, [ADI25, Definition 3.4]). A designated-verifier succinct non-interactive argument for a relation R, with message length ℓ, is a triple $(\mathsf{Setup},\mathsf{P},\mathsf{V})$: Setup on input 1^n outputs a common reference string crs and a verification state st; $\mathsf{P}(\mathsf{crs},x,w)$ outputs $\mathsf{pf}\in\{0,1\}^\ell$; and $\mathsf{V}(st,x,\mathsf{pf})$ outputs a bit. All three have access to the generic group oracle. It has *completeness error* α if for all $(x,w)\in R$,

$$\Pr\left[\mathsf{V}^G(st,x,\mathsf{pf})=1\right]\geq 1-\alpha(\lambda,|x|),$$

over $G\leftarrow\mathsf{GGM}(\lambda)$, $(\mathsf{crs},st)\leftarrow\mathsf{Setup}^G(1^{|x|})$ and $\mathsf{pf}\leftarrow\mathsf{P}^G(\mathsf{crs},x,w)$. It has *adaptive soundness error* δ if for every prover P' making at most t oracle queries,

$$\Pr\left[x\notin L(R)\ \wedge\ \mathsf{V}^G(st,x,\mathsf{pf})=1\right]\leq\delta(\lambda,|x|,t),$$

over $G\leftarrow\mathsf{GGM}(\lambda)$, $(\mathsf{crs},st)\leftarrow\mathsf{Setup}^G(1^{|x|})$ and $(x,\mathsf{pf})\leftarrow\mathsf{P}'^G(\mathsf{crs})$. It is *succinct* if $|\mathsf{pf}|=o(|w|)$.

Conjecture 1 ([ADI25, Conjecture 1.3]). *Let $\mathbb{G}=\mathbb{G}_\lambda$ be a generic group and τ a soundness parameter. There exists a dv-SNARG (Definition 2) for proving the satisfiability of a Boolean circuit of size s with the following features:*

- *soundness error* $2^{-\tau+\log\log\lambda} + O(t^2/2^\lambda)$ *against t-query adversaries;*
- *proof size* 1 $\mathbb{G}$*-element and* $\tau + o(\tau)$ *additional bits;*
- *CRS size* $O(\tau s)$ $\mathbb{G}$*-elements.*

Remark 1 (No random oracle). Conjecture 1 lives in the generic group model alone. This matters, because the source's better concrete bound (Theorem 1.2, one $\mathbb{G}$-element, one random-oracle output and about 2τ bits) buys its tighter malleability analysis with a random oracle, and its random-oracle-free theorem (Theorem 1.1) pays $O(\tau)$ bits with a large hidden constant — 56τ bits once the CRS is allowed to be $O(\tau s^2)$. The conjecture asks for $\tau + o(\tau)$ bits with a *linear* CRS and no oracle beyond the generic group.

Remark 2 (The two ingredients the source names). The source presents Conjecture 1 as what its two identified improvements "could lead to". Neither is established: a tighter malleability analysis of packed ElGamal in the generic group model, for which the source gives an explicit candidate construction it conjectures achieves soundness $2^{-\tau}$ with one group element and about 2τ bits; and a practical linear PCP with answer-to-soundness ratio $\mu \approx 1$, which the source leaves open. A resolution of Conjecture 1 need not go through either, but a resolution of neither ingredient plus a proof of the conjecture would be a surprise.

Remark 3 (The soundness term is unusual and is the source's). The $\log\log\lambda$ in the exponent is written as in the source: the conjectured soundness error is $2^{-\tau+\log\log\lambda} + O(t^2/2^\lambda)$, so the conjecture allows a $\log\lambda$ multiplicative loss over $2^{-\tau}$. It is not a typographical slip introduced here, and a construction achieving $2^{-\tau}$ exactly would be stronger than what is asked.

Remark 4 (Neighbouring open problems, not this one). The source lists two further directions that are not part of Conjecture 1: reducing prover and verifier runtimes — where it conjectures separately (its Conjecture 3.11) that its LPCP is $O(\lambda p^2 s)$-bounded, which would let a random-walk concentration bound cut verification time — and achieving full CRS reusability against a prover who observes every accept/reject decision. Both are distinct statements.

4 Bibliography

[ADI25] Gal Arnon, Jesko Dujmovic and Yuval Ishai. *Designated-verifier SNARGs with one group element.* IACR ePrint 2025/517. The source. Conjecture 1.3 is on page 6; Theorem 1.1 on page 4, Theorem 1.2 on page 5; Definitions 3.2 and 3.4 on pages 14–15.

[BIOW20] Ohad Barta, Yuval Ishai, Rafail Ostrovsky and David J. Wu. *On succinct arguments and witness encryption from groups.* CRYPTO 2020. The two-group-element dv-SNARG with inverse-polynomial soundness the source improves on, and the source of one of the linear PCPs it uses.

[BCI+13] Nir Bitansky, Alessandro Chiesa, Yuval Ishai, Rafail Ostrovsky and Omer Paneth. *Succinct non-interactive arguments via linear interactive proofs.* TCC 2013, LNCS 7785, pages 315–333. The linear-only-encryption compiler the source extends to compressible encryption.

[BHI+24] Nir Bitansky, Prahladh Harsha, Yuval Ishai, Ron D. Rothblum and David J. Wu. *Dot-product proofs and their applications.* 65th Annual Symposium on Foundations of Computer Science (FOCS), 2024, pages 806–825. The 1-query linear PCP the source uses for a linear-size CRS, and the work that observes that hardness-of-approximation for MAXLIN yields LPCPs with $\mu \approx 1$.

[Gro16] Jens Groth. *On the size of pairing-based non-interactive arguments.* EUROCRYPT 2016, Part II, LNCS 9666, pages 305–326. The pairing-based SNARG whose proof size the source's concrete count is compared against.

[Has01] Johan Håstad. *Some optimal inapproximability results.* Journal of the ACM, 48(4):798–859, 2001. The optimal MAXLIN inapproximability the $\mu \approx 1$ LPCPs come from.

[BGI17] Elette Boyle, Niv Gilboa and Yuval Ishai. *Group-based secure computation: optimizing rounds, communication, and computation.* EUROCRYPT 2017, Part II, LNCS 10211, pages 163–193. The distributed discrete logarithm algorithm the source's packed ElGamal decryption uses, which is what gives it perfect completeness.