AICR · OPEN PROBLEM

Somewhere Statistically Sound Arguments Are Fiat-Shamir Friendly

A class that evades every known Fiat-Shamir counterexample — conjecturally, for a reason

Status. Statement: AI-written from Yael Tauman Kalai, Vinod Vaikuntanathan and Rachel Yun Zhang, *Somewhere Statistical Soundness, Post-Quantum Security, and SNARGs*, IACR ePrint 2021/788. Not yet checked by a human. This is their Conjecture 1.3. They are explicit that they do not prove it — "We emphasize that we do not prove that any SSS interactive argument is Fiat-Shamir friendly, only conjecture it" — and ask for "the proof (or refutation) of this conjecture" as "an important open problem." They do prove that SSS implies straight-line soundness, hence post-quantum soundness.

Category. *Proof Systems.*

Conjecture (informal). *The Fiat-Shamir transform turns an interactive protocol into a non-interactive one by replacing the verifier's coins with a hash of the transcript. It is used everywhere and it is not sound in general: there are interactive arguments for which it fails no matter which hash family is used, and Kilian's protocol is among them. Look at how those counterexamples are built and they all share a trick — an extra accepting clause that a prover who can predict the verifier's next message can exploit. That clause is precisely what destroys statistical soundness on any fixed slice of the protocol. The source isolates the class of arguments that keep such a slice, calls them somewhere statistically sound, and conjectures that no counterexample can live there.*

1 The setting

Fiat-Shamir is sound for constant-round *proofs* — statistically sound protocols — but for *arguments*, where soundness holds only against efficient provers, there are counterexamples that hold no matter which hash family is used, and more recently it was shown that the

paradigm is not sound when applied to Kilian's protocol.

The source introduces a hybrid class sitting between the two. Informally, in a 4-round protocol where the verifier speaks first, the argument is somewhere statistically sound if for every first verifier message there is a distinguished third message such that, conditioned on the first three messages being that pair plus whatever the prover said in between, the rest of the protocol is statistically sound. The name is by analogy with somewhere statistical binding: soundness holds statistically on a hidden slice, and computationally elsewhere.

Two things the source proves about the class, which are the reason to care about it independently of the conjecture. Its Theorem 4.3: any θ-SSS interactive argument with respect to a θ-decisional complexity assumption is θ-straight-line sound — and hence post-quantum sound if the underlying assumption is. And it proves that its own instantiation of Kilian's protocol, with a multi-extractable somewhere statistically binding hash family and a BMW-compatible PCP, is SSS.

2 Notation and parameters

- κ is the security parameter; $(\mathcal{P},\mathcal{V})$ is an interactive argument for a language L.
- $\theta = \theta(\kappa)$ parameterizes the soundness error and the adversary size: a protocol is *θ-statistically sound* if its soundness error is at most θ.
- β_1 is the verifier's first message; $T(\beta_1)$ is the distinguished later verifier message the definition quantifies over.
- *Constant round* is the hypothesis of the conjecture. The source's exposition focuses on 4-round protocols with the verifier speaking first, noting the notion extends to multi-round protocols.

3 The conjecture

Definition 1 (Somewhere statistically sound, [KVZ21, Definition 4.2]). An interactive argument $(\mathcal{P},\mathcal{V})(1^\kappa)$ for L is *θ-somewhere statistically sound* with respect to a θ-decisional complexity assumption A if for every first verifier message

β_1 there exists a second verifier message $T(\beta_1)$ such that: for every poly(θ)-size cheating prover $\mathcal{P}^*$ that generates an instance x, conditioned on the first three messages being $(\beta_1, \mathcal{P}^*(\beta_1), T(\beta_1))$, the remaining protocol is θ-statistically sound with overwhelming probability $1 - \text{negl}(\theta)$ over β_1, assuming A.

Definition 2 (Fiat-Shamir friendly, [KVZ21, §1.2.2]). An interactive argument $(\mathcal{P}, \mathcal{V})$ is *Fiat-Shamir friendly* if there exists a hash family $\mathcal{H}$ such that applying the Fiat-Shamir paradigm with respect to $\mathcal{H}$ to $(\mathcal{P}, \mathcal{V})$ results in a sound non-interactive argument.

Conjecture 1 ([KVZ21, Conjecture 1.3]). *Any constant round SSS interactive argument $(\mathcal{P}, \mathcal{V})$ is Fiat-Shamir friendly.*

Remark 1 (Note what is and is not being asked). Definition 2 is existential in the hash family: it asks that *some* $\mathcal{H}$ work, not that a natural one does, and not that the same one work for every protocol. So the conjecture is the weakest useful form. It is correspondingly not a claim that Fiat-Shamir as deployed — with a concrete hash function — is sound for SSS arguments.

Remark 2 (The evidence, which is structural). The source's argument for the conjecture is that all known negative results for Fiat-Shamir are for arguments that are not SSS, and not by accident. Those counterexamples are built by adding an accepting clause such that a prover who can predict the verifier's next message can convince the verifier of a false statement through that clause. In the interactive setting this is harmless, since the prover cannot predict the next message. Under Fiat-Shamir the prover has the hash function and can. And crucially, that clause is exactly what stops the argument from being SSS — its witness is the hash function itself, so the clause inherently lacks statistical soundness on any slice.

There is one positive data point too. Prior to this work the only interactive argument proven Fiat-Shamir friendly, by Canetti et al., "is indeed an SSS argument" — so the class contains the sole known

success as well as excluding all the known failures.

Remark 3 (What a proof would buy, and the sub-goal it would activate). The source's own instantiation of Kilian's protocol is SSS, so Conjecture 1 would imply that instantiation is Fiat-Shamir friendly — in contrast with the result that Kilian's protocol in general is not. More broadly the source proposes "constructing an SSS interactive argument for all of NP as a great open problem," and notes it is easier than constructing a non-adaptive SNARG for NP, since any such SNARG is in particular SSS with two additional arbitrary rounds ignored by the verdict function. So the pair — prove the conjecture, then build a succinct SSS argument for NP — is a proposed route to SNARGs from a standard post-quantum assumption, and the source says it believes it to be a promising one.

Remark 4 (A refutation is a real possibility, and what it would look like). The source predicts a positive answer but proves nothing, and asks for a proof *or a refutation.* A refutation means a constant-round SSS argument together with a proof that no hash family makes Fiat-Shamir sound for it. By Remark 2 such a construction cannot use the extra-accepting-clause trick, so it would have to defeat Fiat-Shamir by a genuinely different mechanism — which is what would make it interesting beyond settling this statement.

Remark 5 (Constant round is a hypothesis). Conjecture 1 is stated for constant-round arguments. The source defines SSS for multi-round protocols as well but focuses its exposition on the 4-round case, and its conjecture carries the constant-round restriction; nothing here should be read as a claim about polynomially many rounds.

4 Bibliography

[KVZ21] Yael Tauman Kalai, Vinod Vaikuntanathan and Rachel Yun Zhang. *Somewhere statistical soundness, post-quantum security, and SNARGs.* IACR ePrint 2021/788. The source. Conjecture 1.3 is on page 8, the informal statement and the discussion of the evidence on page 6, Definition 4.2 on page 21 and Theorem 4.3 on page 22.

[BBH+19] James Bartusek, Liron Bronfman, Justin Holmgren, Fermi Ma and Ron Rothblum. *On the (in)security of Kilian-based SNARGs.* TCC 2019. Shows that Fiat-Shamir applied to Kilian's protocol is in general

not sound, and suggested using a somewhere statistically binding hash family as one step to evade the result. [UNVERIFIED] — cited in the source as [BBH+ 19]; the bibliographic detail here is inferred.

[CSW20] Ran Canetti, Pratik Sarkar and Xiao Wang. *Blazing fast OT for three-round UC OT extension.* Cited by the source as the work giving the only interactive argument previously proven Fiat-Shamir friendly, used to construct a non-succinct UC NIZK for NP with adaptive soundness — and which the source observes is itself an SSS argument. [UNVERIFIED] — cited in the source as [CSW20]; the bibliographic detail here is inferred and may name the wrong paper by these authors.

[Kil92] Joe Kilian. *A note on efficient zero-knowledge proofs and arguments.* STOC 1992. The protocol whose SSS instantiation the source builds, and whose general Fiat-Shamir insecurity the conjecture would be consistent with.

[CMSZ21] Alessandro Chiesa, Fermi Ma, Nicholas Spooner and Mark Zhandry. *Post-quantum succinct arguments.* Cited by the source for resolving the post-quantum soundness of the classical Kilian protocol for all of NP, which the source contrasts with the straight-line route SSS provides. [UNVERIFIED] — cited in the source as [CMSZ21]; the bibliographic detail here is inferred.