**CONJURA · OPEN PROBLEM**

# *Perfect Fully Anonymous Secret Sharing for the 3-out-of-5 Threshold*

*Uniform unauthorized shares, identity-free reconstruction, no error at all*

**Status**. Statement: AI-written from Allison Bishop, Matthew Green, Yuval Ishai, Abhishek Jain and Paul Lou, *Fully Anonymous Secret Sharing*, IACR ePrint 2025/1984. Not yet checked by a human. The statistical and computational versions are settled by the source and by prior work; the perfect version is stated by the source to be open for every reconstruction threshold $3 \le t \le n-2$, and open even for the weaker multi-dealer notion, with 3-out-of-5 singled out as the smallest open case. Con has settled the perfect case for gap threshold structures, where the reconstruction threshold exceeds the secrecy threshold by roughly a factor of two.

**Category**. *Secret Sharing.*

**Conjecture (informal).** *Ordinary secret sharing hides the secret from unauthorized sets of parties, but not much else: the shares may reveal who holds them, and reconstruction may need to know which party contributed which share. Fully anonymous secret sharing asks for both to go away — shares of any unauthorized set look like uniformly random strings, revealing neither party identities nor even whether they came from the same dealer, and reconstruction works from an unordered bag of shares. Shamir's scheme over a large field with random interpolation points almost does this for thresholds, but only almost: it either loses perfect correctness (if the points may repeat) or perfect uniformity (if they are forced distinct), and either way the share size has to grow with the security parameter. A truly perfect scheme would have shares whose size depends on the access structure alone. The source asks whether one exists, and observes that the question is open already for 3-out-of-5.*

## 1 The setting

The source defines three strengths of anonymity for the shares of an unauthorized set, on top of the requirement (going back to Blundo

and Stinson [BS97]) that reconstruction not take party identities as input. *U-anonymity*, the strongest, asks that the shares of any unauthorized set be uniform on the publicly known share domain. *M-anonymity* asks only that a set of unauthorized shares drawn from one sharing be indistinguishable from one where a single share comes from an independent sharing of a possibly different secret — so a mixture of dealers cannot be detected. *S-anonymity*, the weakest, asks only that unauthorized sets of equal size be indistinguishable within one sharing. U-anonymity implies M-anonymity implies S-anonymity, and a scheme with anonymous reconstruction satisfying the respective notion is called U-FASS, M-FASS or S-FASS.

For threshold structures the known route to U-FASS is a large-field variant of Shamir's scheme with random interpolation points, and the source spells out why it is not perfect: if the points are drawn independently, correctness fails when two coincide; if they are forced distinct, the shares are no longer uniform. Either way the share size has to grow with the security or correctness parameter, whereas a perfect U-FASS scheme must achieve anonymity with share size depending only on the access structure.

The source's positive results are statistical or computational: an improved statistical U-FASS for DNF-representable structures, a compiler from any secret-sharing scheme to computational M-FASS from compute-and-compare obfuscation, a U-FASS for complete bipartite graphs from the Decisional Linear assumption, and one for star graphs from one-way functions. Its negative results include an $\Omega(\ell)$ per-party lower bound for a family with many minterms, applying to U-FASS and M-FASS alike and also under imperfect anonymity.

The perfect case is what it records as its first open question: "The first open question is the possibility of perfect U-FASS for general access structures, namely U-FASS with both perfect uniformity and perfect correctness. The question is open even for threshold structures with reconstruction threshold $3 \le t \le n-2$ and even for the weaker notion of perfect M-FASS. In particular, it is open in the 3-out-of-5 threshold case." It also names the state of progress: Con [Con24] shows Shamir's original scheme can be instantiated to give perfect U-FASS for *gap* threshold structures, where the reconstruction threshold exceeds the secrecy threshold by roughly a factor of two — which is exactly why the interesting range is

$3 \le t \le n-2$ and why 3-out-of-5 is the smallest case left.

## 2 Notation and parameters

- $[n] = \{1, \dots, n\}$ is the party set; $\Gamma \subseteq 2^{[n]}$ a monotone access structure. The $t$-out-of-$n$ threshold structure is $\Gamma = \{A : |A| \ge t\}$.
- $\mathcal{S}$ is the secret space, $\lambda$ the security parameter.
- $\Omega_\lambda$ is the efficiently samplable, publicly known support of a single share over all choices of secret — the domain the uniformity requirement compares against.
- $sh \leftarrow \mathsf{Share}(1^\lambda, s)$ produces the share vector; $sh_A = (sh_i)_{i \in A}$; $\mathsf{Recon}(1^\lambda, sh)$ takes shares with no party identities.
- $\mu$ is the anonymity error. *Perfect* means $\mu = 0$ and, for correctness, error exactly 0.

## 3 The conjecture

**Definition 1 (Anonymous reconstruction, [BGIJL25, Definition 3.5], after [BS97]).** A secret-sharing scheme with anonymous reconstruction for $\Gamma$ and secret space $\mathcal{S}$ is a pair $(\mathsf{Share}, \mathsf{Recon})$ where $\mathsf{Share}(1^\lambda, s)$ is randomized and $\mathsf{Recon}(1^\lambda, sh)$ is deterministic and takes *only* a tuple of shares — no party identities. It is *perfectly correct* if for every $\lambda$, every $s \in \mathcal{S}_\lambda$ and every $A \in \Gamma$, $\mathsf{Recon}(1^\lambda, sh_A) = s$ with probability 1 over $sh \leftarrow \mathsf{Share}(1^\lambda, s)$.

**Definition 2 (Uniformity, [BGIJL25, Definition 4.1]).** A scheme $(\mathsf{Share}, \mathsf{Recon})$ for $\Gamma$ is *$\mu$-U-anonymous* (statistically) if for every computationally unbounded $\mathcal{A}$, all large enough $\lambda$, every secret $s \in \mathcal{S}_\lambda$ and every unauthorized $B \in 2^{[n]} \setminus \Gamma_\lambda$,

$$\left| \Pr_{sh \leftarrow \mathsf{Share}(1^\lambda, s)} \left[ \mathcal{A}(1^\lambda, s, B, sh_B) = 1 \right] - \Pr_{U \sim \mathsf{Unif}(\Omega_\lambda)^{|B|}} \left[ \mathcal{A}(1^\lambda, s, B, U) = 1 \right] \right| \le \mu(\lambda$$

where $\Omega_\lambda$ is the publicly known support of a single share. A scheme satisfying Definition 1 together with U-anonymity is a *U-FASS* scheme; it is *perfect* if it is perfectly correct and 0-U-

anonymous.

**Definition 3 (Multi-dealer anonymity, [BGIJL25, Definition 4.2]).** A scheme is $\mu$-*M-anonymous* if for every computationally unbounded $\mathcal{A}$, all large enough $\lambda$, every unauthorized $B$, every $B' \subset B$ with $|B'| = |B| - 1$, every singleton unauthorized $\{a\}$ and all $s_0, s_1 \in \mathcal{S}_\lambda$, the distinguishing advantage between $sh^{(0)}_B$ and $sh^{(0)}_{B'} \| sh^{(1)}_{\{a\}}$ — where $sh^{(0)} \leftarrow \mathsf{Share}(1^\lambda, s_0)$ and $sh^{(1)} \leftarrow \mathsf{Share}(1^\lambda, s_1)$ independently — is at most $\mu(\lambda)$. An M-FASS scheme is *perfect* if it is perfectly correct and 0-M-anonymous. Perfect U-FASS implies perfect M-FASS.

**Conjecture 1 (Perfect FASS at 3-out-of-5).** *There is a perfect M-FASS scheme (Definitions 1 and 3) for the 3-out-of-5 threshold access structure with $|\mathcal{S}| \geq 2$, in which the share domain $\Omega$ and hence the share size depend only on the access structure and the secret space, not on any security or correctness parameter.*

**Remark 1 (Why the weaker notion, and what a positive answer at the stronger one would mean).** The source states the question for perfect U-FASS and adds that it is open "even for the weaker notion of perfect M-FASS". Conjecture 1 is therefore stated at the weaker notion, which is the easier target and the one whose resolution the source flags as already unknown: a perfect M-FASS scheme for 3-out-of-5 settles the weaker question, and a proof that none exists settles the stronger one too, since perfect U-FASS implies perfect M-FASS. A construction achieving perfect U-FASS is strictly better than what is asked here and should be reported as such.

**Remark 2 (Both directions are open).** Nothing in the source predicts an answer. A resolution is either such a scheme or a proof that no perfect M-FASS scheme for 3-out-of-5 exists with parameter-independent share size. The source's own $\Omega(\ell)$ lower bound does not apply: it is for an access structure with many minterms, and it explicitly does not cover the single-minterm and small-threshold cases.

**Remark 3 (What "perfect" rules out).** The constant-share-size clause in Conjecture 1 is the source's own reading of what perfect

means here: "a perfect U-FASS scheme must provide anonymity with *constant-size* shares, depending only on the access structure." It is what excludes the known threshold construction, whose share size grows with the security or correctness parameter precisely because it must make interpolation-point collisions rare rather than impossible. A scheme with 0 error whose share size still grows with a parameter $\lambda$ would not be a resolution.

**Remark 4 (Neighbouring questions in the same list).** The source's open-questions section also asks for improved information-theoretic FASS for the single-minterm access structure (better than its $\widetilde{O}(t\lambda)$ per-party upper bound, and with efficient reconstruction for a one-bit secret), for information-theoretic S-FASS for weighted threshold structures matching the efficiency of virtualized Shamir, and whether one-way functions suffice for computational U-FASS for CNF — or whether such a scheme implies public-key encryption. None of those is this statement.

# 4 Bibliography

[BGIJL25] Allison Bishop, Matthew Green, Yuval Ishai, Abhishek Jain and Paul Lou. *Fully anonymous secret sharing.* IACR ePrint 2025/1984. The source. Definitions 3.5, 4.1 and 4.2 are on pages 19, 23–24; the open question is the first item of Section 2.4 ("Open Questions and Future Directions"), page 17.

[BS97] Carlo Blundo and Douglas R. Stinson. *Anonymous secret sharing schemes.* Discrete Applied Mathematics, 77(1):13–28, 1997. The anonymous-reconstruction syntax the source's Definition 3.5 adopts.

[Con24] Roni Con. *Anonymous Shamir's secret sharing via Reed–Solomon codes against permutations, insertions, and deletions.* arXiv 2412.17003, 2024; presented at ISIT 2025. The recent progress the source credits: Shamir's original scheme can be instantiated to give a perfect U-FASS scheme for gap threshold structures, where the reconstruction threshold is bigger than the secrecy threshold by roughly a factor of 2.

[Sha79] Adi Shamir. *How to share a secret.* Communications of the ACM, 22(11):612–613, November 1979. The threshold scheme whose large-field random-interpolation-point variant is the known U-FASS for thresholds.