

Weakly Private $(n-1)$ -out-of- n Secret Sharing Below Logarithmic Share Size

Perfect correctness, deniability instead of secrecy, a one-bit secret

Status. Statement: AI-written from Amos Beimel, Yuval Ishai, Eyal Kushilevitz and Hanjun Li, *Cryptography with Weak Privacy*, IACR ePrint 2025/1978. Not yet checked by a human. The 2-out-of- n case is settled: Beimel and Franklin give $1/n$ -weakly-private schemes with share size 2, against $\Theta(\log n)$ for perfect privacy. Large thresholds are stated by the source to be open, and it asks specifically about $(n-1)$ -out-of- n at share size $o(\log n)$.

Category. *Secret Sharing.*

Conjecture (informal). *Weak privacy asks far less of a secret-sharing scheme than secrecy does: not that an unauthorized set learn nothing, only that it cannot rule out any secret — formally, that the probability of any view under one secret is at least p times its probability under any other. The point of the relaxation is that it is combinatorial, so lower bounds for it are usually easy, and strong upper bounds for it therefore rule out combinatorial routes to the notoriously stuck lower bounds for perfect secret sharing. Beimel and Franklin showed the relaxation buys a lot at the low end: 2-out-of- n threshold sharing of a bit needs $\Theta(\log n)$ bits per share with perfect privacy, but only 2 bits with weak privacy. The source asks what happens at the other end of the threshold range: can $(n-1)$ -out-of- n weakly private sharing of a bit be done with share size $o(\log n)$?*

1 The setting

For a monotone access structure, the gap between the best known lower bound on share size, $\Omega(n/\log n)$ [Csirmaz94], and the best known upper bounds is exponential, and has stayed so through recent progress. The source proposes weak privacy as a tractable toy version of the same questions: keep perfect correctness, replace secrecy by the requirement that no admissible secret be ruled out, and see whether the exponential gaps close.

Its definition is a reparameterized pure differential privacy. A scheme is *p-weakly private* (*p*-WP) if for every unauthorized set A , every pair of secrets and every vector of shares for A , the probability of those shares under the first secret is at least p times their probability under the second; *p*-WP with $p = 1$ is perfect privacy, and *p*-WP corresponds to ε -differential privacy with $\varepsilon = \ln(1/p)$. Unlike in differential privacy, the interesting regime here is small p , and unlike in differential privacy, the comparison is over *all* pairs of secrets rather than neighbouring ones.

The relaxation is known to be powerful at the low end of the threshold range. Beimel and Franklin [BF07] construct $1/n$ -WP 2-out-of- n threshold schemes with share size 2 for a one-bit secret, against the $\Theta(\log n)$ share size that perfect privacy requires for the same access structure [Shamir79, Blakley79, KN90, CCX13]. The source’s own positive results are for general access structures and for various restricted families, and its negative results transfer a known lower-bound technique to the WP setting for decomposable randomized encodings.

What it does not settle is large thresholds. Its “Open Problems” list reads: “Beimel and Franklin [9] constructed $1/n$ -WP 2-out-of- n threshold secret-sharing schemes with share size 2, leaving the case of large thresholds open. Is there a WP $(n - 1)$ -out-of- n threshold secret-sharing scheme with share size $o(\log n)$?”

2 Notation and parameters

- $P = \{p_1, \dots, p_n\}$ is the party set. For $1 \leq t \leq n$, the *t-out-of-n threshold* access structure has $\Gamma_{\text{yes}} = \{A \subseteq P : |A| \geq t\}$ and $\Gamma_{\text{no}} = \{A \subseteq P : |A| < t\}$.
- $\mathcal{S}$ is the domain of secrets, with $|\mathcal{S}| \geq 2$; $\mathcal{S}_1, \dots, \mathcal{S}_n$ the domains of shares.
- The *size of the secret* is $\log |\mathcal{S}|$, the *share size of party* p_j is $\log |\mathcal{S}_j|$, and the *max share size* is $\max_j \log |\mathcal{S}_j|$. Share size below means max share size.
- $p \in (0, 1]$ is the weak-privacy parameter, and may depend on n .

3 The conjecture

Definition 1 (Weakly private secret sharing, [BIKL25, Definition 2.2]). A secret-sharing scheme is a randomized mapping Π taking a secret $s \in \mathcal{S}$ to a tuple $\langle sh_1, \dots, sh_n \rangle \in \mathcal{S}_1 \times \dots \times \mathcal{S}_n$; for $A \subseteq P$, $\Pi_A(s)$ is its restriction to the entries of A . For $0 < p \leq 1$, Π is a p -WP secret-sharing scheme realizing $\Gamma = (\Gamma_{\text{no}}, \Gamma_{\text{yes}})$ if

- *perfect correctness*: for every $B = \{p_{i_1}, \dots, p_{i_{|B|}}\} \in \Gamma_{\text{yes}}$ there is a reconstruction function $\text{Recon}_B : \mathcal{S}_{i_1} \times \dots \times \mathcal{S}_{i_{|B|}} \rightarrow \mathcal{S}$ with $\text{Recon}_B(\Pi_B(s)) = s$ for every $s \in \mathcal{S}$ and every choice of Π 's randomness; and
- *p -weak privacy*: for every $A \in \Gamma_{\text{no}}$, all $s_1, s_2 \in \mathcal{S}$ and every share vector $\langle sh_j \rangle_{p_j \in A}$,

$$\Pr[\Pi_A(s_1) = \langle sh_j \rangle_{p_j \in A}] \geq p \cdot \Pr[\Pi_A(s_2) = \langle sh_j \rangle_{p_j \in A}].$$

A scheme is *weakly private* if it is p -WP for some $p > 0$.

Conjecture 1 (Sub-logarithmic weakly private sharing at threshold $n - 1$). *There is a family of weakly private secret-sharing schemes (Definition 1), one for each n , realizing the $(n - 1)$ -out-of- n threshold access structure with a one-bit secret ($|\mathcal{S}| = 2$) and max share size $o(\log n)$.*

Remark 1 (Both directions are open). The source states this as a question. A resolution is either such a family — for some $p = p(n) > 0$, with no requirement that p be inverse-polynomial — or a proof that every weakly private $(n - 1)$ -out-of- n scheme for a one-bit secret has max share size $\Omega(\log n)$. The second direction would be a lower bound in the weak model, which is precisely where the source expects lower bounds to be easier than in the perfect model, and where an obstruction found would be informative about the perfect case too.

Remark 2 (Where the privacy parameter sits). Definition 1 quantifies over a fixed p , and the source's 2-out-of- n benchmark is $1/n$ -WP with share size 2. The question as the source poses it asks for weak privacy without pinning p , so Conjecture 1 does likewise: any

$p > 0$ counts, and a resolution should state the p it achieves. Note that a scheme is only interesting here if p does not itself smuggle in the share size — Definition 1 allows p to be exponentially small, but perfect correctness with max share size $o(\log n)$ is the binding constraint.

Remark 3 (Why the threshold matters, not just the gap). At threshold 2 an unauthorized set is a single party, and weak privacy need only be maintained against one share. At threshold $n - 1$ an unauthorized set is any $n - 2$ parties, so almost all shares are seen at once while perfect correctness must still hold for every set of $n - 1$. That is what makes the case qualitatively different from Beimel and Franklin’s, and it is why the source records the large-threshold case as open rather than as a variant of the small one. The source’s separate question about *general* access structures — whether weakly private schemes with share size $o(n)$ exist for arbitrary access structures — is not this statement.

4 Bibliography

- [BIKL25] Amos Beimel, Yuval Ishai, Eyal Kushilevitz and Hanjun Li. *Cryptography with weak privacy*. IACR ePrint 2025/1978. The source. Definition 2.2 is on page 12; the open problem is the last item of the “Open Problems” list, page 7.
- [BF07] Amos Beimel and Matthew K. Franklin. *Weakly-private secret sharing schemes*. Fourth Theory of Cryptography Conference (TCC), 2007, LNCS 4392, pages 253–272. The $1/n$ -WP 2-out-of- n scheme with share size 2, and the case the source’s question generalizes away from.
- [Csirmaz94] László Csirmaz. *The size of a share must be large*. EUROCRYPT 1994, LNCS 950, pages 13–22. The $\Omega(n/\log n)$ lower bound on share size for perfect secret sharing, the bound whose distance from the upper bounds motivates the source’s programme.
- [Shamir79] Adi Shamir. *How to share a secret*. Communications of the ACM, 22:612–613, 1979. Threshold secret sharing with perfect privacy.
- [Blakley79] George Robert Blakley. *Safeguarding cryptographic keys*. 1979 AFIPS National Computer Conference, AFIPS Conference Proceedings volume 48, pages 313–317. The other original threshold construction.

- [KN90] Joe Kilian and Noam Nisan. Private communication, 1990. One of the sources the paper credits for the $\Theta(\log n)$ share size required by perfectly private 2-out-of- n sharing.
- [CCX13] Ignacio Cascudo, Ronald Cramer and Chaoping Xing. *Bounds on the threshold gap in secret sharing and its applications*. IEEE Transactions on Information Theory, 59(9):5600–5612, 2013. Threshold-gap bounds, cited by the source alongside the above for the perfect-privacy share size.