CONJURA · OPEN PROBLEM

The Exact Randomness Complexity of t-Secure XOR

$\Omega(t^2)$ from below, $O(t^2 \log(n/t))$ from above — which is it?

Status. Statement: AI-written from Vipul Goyal, Yuval Ishai and Yifan Song, *Tight Bounds on the Randomness Complexity of Secure Multiparty Computation*, IACR ePrint 2022/799. Not yet checked by a human. The source proves an $\Omega(t^2)$ lower bound, matching Kushilevitz and Mansour's non-explicit $O(t^2 \log(n/t))$ upper bound up to a logarithmic factor — and up to a constant factor when $t = \Omega(n)$ — and gives an explicit protocol at $O(t^2 \log^2 n)$. It states it leaves the remaining polylogarithmic gaps open.

Category. *Secure Multiparty Computation.*

Conjecture (informal). *Randomness is a resource like any other, and for information-theoretic secure computation it is one of the few whose exact cost might actually be determined. Take the simplest interesting function: n parties each holding a bit want the XOR of all of them, with privacy against any t of them colluding. The textbook protocol tosses $O(nt)$ coins. Kushilevitz and Mansour cut that to $O(t^2 \log(n/t))$, but non-explicitly, and could only prove $\Omega(t)$ necessary. The source closes most of that quadratic gap, proving $\Omega(t^2)$ coins are necessary and giving an explicit protocol using $O(t^2 \log^2 n)$. What is left is the polylogarithmic factor between them, and the source says it leaves that open.*

1 The setting

In the standard model of information-theoretic MPC, n parties each holding an input from a finite domain run a protocol computing f, every party learning the output, with privacy against any t colluding parties. Each party may toss coins as needed, and the *randomness complexity* of the protocol is the total number of coins tossed in the worst case.

For XOR — or more generally addition over a finite abelian group — the textbook protocol of Benaloh and of Chor and Kushile-

vitz uses $O(nt)$ coins for any $t < n$. Kushilevitz and Mansour improved the upper bound to $O(t^2 \log(n/t))$ and proved $\Omega(t)$ necessary, leaving a quadratic gap; their protocol is non-explicit, resting on a combinatorial object obtainable either by an efficient probabilistic construction with small failure probability or deterministically in super-polynomial time, and they also left the existence of an explicit protocol matching their bound open. Blundo et al. obtained $\Omega(t^2/(n-t))$, which the textbook protocol matches when $t = n - \Omega(1)$ but which still leaves a quadratic gap for $t \le (1-\varepsilon)n$.

The source settles the main questions. It proves an $\Omega(t^2)$ lower bound for XOR, extending to arbitrary symmetric Boolean functions including AND and majority, and holding also when the output goes to a strict subset of the parties and when extra input-less participants are present. It gives an explicit protocol for XOR using $O(t^2 \log^2 n)$ coins, extends it to symmetric Boolean functions and to addition over any finite abelian group, and shows t additions cost only $\widetilde{O}(t^2)$ — essentially the price of one. For general circuits it gets $O(t^2 \log |C|)$, but in the easier setting that permits input-less helper parties.

Its lower bound is deliberately combinatorial rather than information-theoretic, and the source explains why it must be: with statistical rather than perfect privacy, a folklore protocol picks a random committee of σ parties and secret-shares among them, achieving $2^{-\Omega(\sigma)}$ security against $t = 0.99n$ corruptions with only $O(n\sigma)$ coins — beating any $\Omega(n^2)$ bound once $\sigma = o(n)$. So the statement below is about perfect privacy.

What remains is the gap between $\Omega(t^2)$ and the upper bounds. The source records: “We leave open the question of characterizing the randomness complexity of general MPC without helper parties, as well as closing the remaining (polylogarithmic) gaps between our lower bounds and upper bounds.” It also names a reason for pessimism: Kushilevitz et al. showed a two-way relation between the randomness complexity of f at $t = 1$ and the circuit complexity of f.

2 Notation and parameters

- n is the number of parties, each holding one bit; f is XOR, $f(x_1, \ldots, x_n) = x_1 \oplus \cdots \oplus x_n$.

- $t < n$ is the privacy threshold: the protocol is t-secure if any t colluding parties learn nothing beyond the output.
- The *randomness complexity* is the total number of coins tossed by all parties in the worst case over inputs and coins.
- Privacy is *perfect*: the joint view of any t parties is identically distributed for all inputs consistent with the output. Remark 3 explains why this may not be relaxed.
- A protocol is *explicit* if its description is computable in polynomial time, as opposed to resting on a combinatorial object obtained probabilistically or in super-polynomial time.

3 The conjecture

Definition 1 (Randomness complexity of t-secure XOR). Let $\mathrm{RC}(n,t)$ denote the least r for which there is an n-party protocol computing XOR with perfect t-security in which at most r coins are tossed in total, in the worst case. Let $\mathrm{RC}^*(n,t)$ denote the same quantity restricted to explicit protocols.

Theorem 1 (What is known). $\mathrm{RC}(n,t) = \Omega(t^2)$ *(the source), and* $\mathrm{RC}(n,t) = O(t^2 \log(n/t))$ *non-explicitly (Kushilevitz and Mansour), and* $\mathrm{RC}^*(n,t) = O(t^2 \log^2 n)$ *(the source). When* $t = \Omega(n)$ *the first two match up to a constant factor.*

Conjecture 1 (The exact order). *Determine the order of* $\mathrm{RC}(n,t)$ *for* $t = o(n)$*, by resolving one of the following:*

(a) $\mathrm{RC}(n,t) = \Theta(t^2)$*, i.e. there is a protocol computing* XOR *with perfect* t*-security using* $O(t^2)$ *coins; or*

(b) $\mathrm{RC}(n,t) = \omega(t^2)$*, i.e. the* $\Omega(t^2)$ *lower bound can be improved, for some* $t = o(n)$*.*

Remark 1 (Why $t = o(n)$, and why the regime matters). For $t = \Omega(n)$ the source's lower bound and Kushilevitz and Mansour's upper bound already agree up to a constant factor, so there is nothing asymptotic left to settle there. The open regime is t genuinely sublinear in n, where the upper bound's $\log(n/t)$ factor is unbounded. Conjecture 1 is stated for that regime for that reason.

Remark 2 (Explicitness is a separate axis). There are two gaps,

not one, and they should not be conflated. The gap between $\Omega(t^2)$ and the *non-explicit* $O(t^2 \log(n/t))$ is Conjecture 1. The further gap up to the source's *explicit* $O(t^2 \log^2 n)$ is the question Kushilevitz and Mansour left open — an explicit protocol matching their bound — which the source improves on without closing. A resolution should say which of the two it settles, and an explicit protocol at $O(t^2 \log(n/t))$ would settle the second without touching the first.

Remark 3 (Perfect privacy is load-bearing). With statistical privacy the question dissolves: the folklore committee-plus-secret-sharing protocol achieves $2^{-\Omega(\sigma)}$ security against $t = 0.99n$ corruptions using $O(n\sigma)$ coins, which beats $\Omega(n^2)$ whenever $\sigma = o(n)$. The source makes exactly this point to explain why its lower-bound technique is combinatorial rather than information-theoretic, and why the information-theoretic technique of Blundo et al. deteriorates as t moves away from n. So Conjecture 1 concerns perfect privacy, and a statistically private protocol below $\Omega(t^2)$ is not a refutation.

Remark 4 (Evidence that this is hard). The source points at Kushilevitz, Ostrovsky and Rosén, who showed a two-way relation between the randomness complexity of f at $t = 1$ and the circuit complexity of f. That is a warning about the general problem rather than about XOR specifically — XOR's circuit complexity is not in doubt — but it is the reason the source gives for expecting the remaining gaps to be difficult in some parameter regimes.

Remark 5 (Neighbouring questions the source also leaves open). Two others, both distinct from this statement: characterizing the randomness complexity of general MPC *without* helper parties, where the source's $O(t^2 \log |C|)$ protocol needs input-less participants; and extending its lower bounds to a more liberal measure in which each party's randomness comes from an arbitrary distribution and the quantity to minimize is entropy rather than a count of coins.

4 Bibliography

[GIS22] Vipul Goyal, Yuval Ishai and Yifan Song. *Tight bounds on the randomness complexity of secure multiparty computation.* IACR ePrint 2022/799. The source. The state of the art and its contribution are on pages 2–3, the statement of what it leaves open on page 3, and the alternative randomness measures in its Appendix B.

[KM97] Eyal Kushilevitz and Yishay Mansour. *Randomness in private computations.* SIAM Journal on Discrete Mathematics, 10(4):647–661, 1997 (earlier version in PODC 1996). The $O(t^2 \log(n/t))$ non-explicit upper bound and the $\Omega(t)$ lower bound, and the source of the explicit-protocol question.

[BDPV99] Carlo Blundo, Alfredo De Santis, Giuseppe Persiano and Ugo Vaccaro. *Randomness complexity of private computation.* Computational Complexity, 8(2):145–168, 1999. The $\Omega(t^2/(n-t))$ information-theoretic lower bound, matched by the textbook protocol when $t = n - \Omega(1)$.

[Ben86] Josh Cohen Benaloh. *Secret sharing homomorphisms: keeping shares of a secret sharing.* CRYPTO '86, pages 251–260. One of the two sources of the textbook $O(nt)$-coin protocol for XOR.

[CK93] Benny Chor and Eyal Kushilevitz. *A communication-privacy tradeoff for modular addition.* Information Processing Letters, 45(4), 1993. The other source of the textbook protocol.

[KOR96] Eyal Kushilevitz, Rafail Ostrovsky and Adi Rosén. *Characterizing linear size circuits in terms of privacy.* STOC 1996, pages 541–550. Shows a two-way relation between randomness complexity at $t = 1$ and circuit complexity, which the source names as evidence for the difficulty of the remaining gaps.

[GIS22a] Vipul Goyal, Yuval Ishai and Yifan Song. *Private circuits with quasilinear randomness.* EUROCRYPT 2022, pages 192–221. The randomness-efficient private-circuit techniques the source's general-circuit protocol builds on.