CONJURA · OPEN PROBLEM

Degree-2 Statistical Randomized Encodings for Every Finite Function

Degree 3 is classical; degree 2 has been open for over twenty years

Status. Statement: AI-written from Benny Applebaum, Zvika Brakerski, Sanjam Garg, Yuval Ishai and Akshayaram Srinivasan, *Separating Two-Round Secure Computation from Oblivious Transfer*, IACR ePrint 2020/116. Not yet checked by a human. The question is not the harvested paper's own: it is Question 1.6 there, attributed to Ishai and Kushilevitz and to Applebaum, Ishai and Kushilevitz, and open since 2000. What the harvested paper adds is a new consequence, its Proposition 1.7. Degree-3 statistical randomized encodings exist for every finite function; negative results are known for *perfectly* private degree 2.

Category. *Information-Theoretic Cryptography.*

Conjecture (informal). *A randomized encoding replaces a function $f(x)$ by a randomized $\hat{f}(x;r)$ whose output determines $f(x)$ and reveals nothing else. The point is that $\hat{f}$ can be far simpler than f, and the natural measure of simplicity is algebraic degree in the indeterminates (x,r). Every finite function has an encoding of degree 3 — that is classical, and it is the reason so much of secure computation reduces to degree-3 objects. Degree 2 is a different matter: with* perfect *privacy it is known to be impossible for some functions, and with a small privacy error allowed, nobody has known the answer since the question was posed in 2000. The harvested paper shows one thing a positive answer would buy: a complete 3-party functionality for two-round black-box MPC, where today only a 4-party one is known.*

1 The setting

A randomized encoding (RE) of f is a randomized $\hat{f}(x;r)$ such that the distribution of $\hat{f}(x)$ determines $f(x)$ and is simulatable from it. The notion, from Ishai and Kushilevitz and developed by Applebaum, Ishai and Kushilevitz, is one of the workhorses of secure computation: it lets a protocol for a complicated f be replaced by a

protocol for a simpler $\hat{f}$. Degree, in the indeterminates (x, r) jointly, is the standard measure of that simplicity, and the classical fact is that every finite f admits an RE of degree 3.

Degree 2 is where it stops. Ishai and Kushilevitz proved negative results for *perfectly* private degree-2 RE. For *statistical* privacy — a small non-zero privacy error permitted — the question has stood open for over twenty years, and the harvested paper records it as Question 1.6, attributing it to Ishai and Kushilevitz and to Applebaum, Ishai and Kushilevitz: "Does every finite function admit a degree-2 statistical randomized encoding?" It adds that the question "has been put forward as a barrier for solving other questions", and a second paper in the same harvest batch — Halevi, Ishai, Kushilevitz and Rabin on additive randomized encodings — independently flags it as "[t]he main open question about RE ... open for over 20 years".

What the harvested paper contributes is a new consequence, in the setting of two-round black-box MPC. For $d \leq p$, let (d, p)-MULTPlus be the p-party functionality in which each of the first d parties holds an input (x_i, z_i) and the product-sum $\prod_i x_i + \sum_i z_i$ over $\mathbb{F}_2$ is delivered to all p parties; standard 2-party OT is equivalent to $(2,2)$-MULTPlus under strict round-preserving black-box (RPBB) reductions. Its Theorem 1.5 shows $(3,4)$-MULTPlus is MPC-complete under strict RPBB reductions: every n-party functionality can be realized using parallel calls to it plus black-box use of a PRG, with no further interaction. Its main negative result rules out any 2-party functionality playing that role. The 3-party case is where Question 1.6 enters, via its Proposition 1.7: "A positive answer to Question 1.6 would imply that Theorem 1.5 holds with $(2,3)$-MULTPlus instead of $(3,4)$-MULTPlus. In particular, it would imply that there is a complete 3-party functionality with respect to strict RPBB reductions."

The same barrier appears twice more in that paper's open problems: extending its negative result from 2-round to 3-round protocols, and proving a negative result for 3-party complete functionalities, would each require settling Question 1.6 *in the negative.*

2 Notation and parameters

- $f : \{0,1\}^n \to \{0,1\}^m$ is a *finite* function — constant input length — which is the regime the question is posed in.
- $\hat{f}(x;r)$ is the encoding; r is its random input. Its *degree* is the total degree of its output coordinates as polynomials over $\mathbb{F}_2$ in the indeterminates (x,r) jointly.
- ε is the privacy error. *Perfect* privacy is $\varepsilon = 0$; *statistical* privacy allows $\varepsilon > 0$ small, and is what makes the question open.
- $\mathrm{SD}(\cdot,\cdot)$ is statistical distance.
- In the consequence, (d,p)-MULTPlus is the p-party product-sum functionality above, and RPBB abbreviates round-preserving black-box.

3 The conjecture

Definition 1 (Randomized encoding of degree d). Let $f : \{0,1\}^n \to \{0,1\}^m$. A randomized function $\hat{f} : \{0,1\}^n \times \{0,1\}^\rho \to \{0,1\}^s$ is an *ε-statistically private randomized encoding* of f if

- *Correctness*: there is a decoder Dec with $\mathrm{Dec}(\hat{f}(x;r)) = f(x)$ for every x and every r; and
- *Privacy*: there is a simulator Sim with $\mathrm{SD}\big(\hat{f}(x;r), \mathrm{Sim}(f(x))\big) \le \varepsilon$ for every x, over uniform r.

It has *degree d* if every output coordinate of $\hat{f}$, viewed as a polynomial over $\mathbb{F}_2$ in the indeterminates (x,r), has total degree at most d. Privacy is *perfect* when $\varepsilon = 0$.

Conjecture 1 (Question 1.6 of [ABGIS20], after [IK00, AIK04]). *Every finite function f admits a degree-2 statistical randomized encoding: for every $\varepsilon > 0$ there is an ε-statistically private randomized encoding of f of degree 2 in the sense of Definition 1.*

Proposition 1 (One consequence, [ABGIS20, Proposition 1.7]). *A positive answer to Conjecture 1 would imply that [ABGIS20, Theorem 1.5] holds with $(2,3)$-MULTPlus in place of $(3,4)$-MULTPlus; in particular, that there is a complete 3-party functionality with respect to strict*

RPBB reductions.

Remark 1 (Attribution: this is not the harvested paper's question). Conjecture 1 is Question 1.6 of the harvested paper, which attributes it to Ishai and Kushilevitz [IK00] and to Applebaum, Ishai and Kushilevitz [AIK04] and describes it as open "for almost 20 years". What the harvested paper adds is Proposition 1.7 and the two barrier observations in its open-problems list. The statement is recorded here because the paper poses it explicitly and supplies new reasons to care, not because it originated there — and a resolution belongs to the older question.

Remark 2 (Why perfect and statistical part company here). Negative results are known for perfectly private degree-2 RE. That does not settle Conjecture 1, and the gap between the two is the whole content of the question: allowing a small privacy error is exactly what the known impossibility arguments do not survive. Anyone attacking the negative direction should expect to need a technique that tolerates error, and anyone attacking the positive direction should not expect perfect correctness to be the obstacle — Definition 1 asks for perfect correctness and only statistical privacy, matching the question as posed.

Remark 3 (Both directions have named consequences). This is unusually well-connected for a twenty-year-old question, and both answers pay. A positive answer gives a complete 3-party functionality for two-round black-box MPC (Proposition 1). A negative answer is what would be *required* to extend the harvested paper's 2-round impossibility to 3-round protocols, and to rule out a 3-party complete functionality — so the paper's own two remaining open problems are blocked on the negative direction specifically.

Remark 4 (The neighbouring ARE question is different). Halevi, Ishai, Kushilevitz and Rabin note that the class of functions admitting statistical degree-2 RE seems *incomparable* to the class admitting statistical additive randomized encodings, even restricting ARE to one input bit per party: the mod-2 inner product trivially has a degree-2 RE but is conjectured to have no ARE, while capped sum has a statistical ARE. So Conjecture 1 is not a reformulation of any ARE question, and progress on one does not automatically transfer.

4 Bibliography

[ABGIS20] Benny Applebaum, Zvika Brakerski, Sanjam Garg, Yuval Ishai and Akshayaram Srinivasan. *Separating two-round secure computation from oblivious transfer.* IACR ePrint 2020/116. The harvested paper. Question 1.6 and Proposition 1.7 are on pages 5–6, Theorem 1.5 and the (d,p)-MULTPlus definition on page 5, and the open-problems list in Section 1.3, pages 9–10.

[IK00] Yuval Ishai and Eyal Kushilevitz. *Randomizing polynomials: a new representation with applications to round-efficient secure computation.* 41st Annual Symposium on Foundations of Computer Science (FOCS), 2000, pages 294–304. Where the question was first posed, and the source of the negative results for perfectly private degree-2 RE.

[AIK04] Benny Applebaum, Yuval Ishai and Eyal Kushilevitz. *Cryptography in NC^0*. 45th Annual Symposium on Foundations of Computer Science (FOCS), 2004, pages 166–175. The other work the harvested paper attributes Question 1.6 to.

[HIKR23] Shai Halevi, Yuval Ishai, Eyal Kushilevitz and Tal Rabin. *Additive randomized encodings and their applications.* IACR ePrint 2023/870. Independently flags this as the main open question about RE, open for over 20 years, and explains why the ARE and degree-2 RE classes are incomparable. [UNVERIFIED] — not in the harvested paper's reference list, being later; read in the Conjura harvest of that paper itself.

[ACJ17] Prabhanjan Ananth, Arka Rai Choudhuri and Abhishek Jain. *A new approach to round-optimal secure multiparty computation.* CRYPTO 2017, Part I, LNCS 10401, pages 468–499. The 4-round black-box protocol the harvested paper contrasts its 2-round impossibility against, leaving the 3-round case open behind the same barrier.

[GIS18] Sanjam Garg, Yuval Ishai and Akshayaram Srinivasan. *Two-round MPC: information-theoretic and black-box.* Theory of Cryptography Conference (TCC) 2018, Part I, pages 123–151. Gives black-box 2-round protocols from group-based primitives with a PKI setup, and the non-black-box construction of client-server 2-round MPC that the harvested paper asks to make black-box.