CONJURA · OPEN PROBLEM

A Perfectly Correct Statistically Secure Additive Randomized Encoding

Statistical security is now known for every function; can the correctness error be removed?

Status. Statement: AI-written from Nir Bitansky, Saroja Erabelli, Rachit Garg and Yuval Ishai, *Shuffling is Universal: Statistical Additive Randomized Encodings for All Functions*, IACR ePrint 2025/1442. Not yet checked by a human. Statistical security with statistical correctness is settled by the source for every finite function; perfect correctness is known in the computational setting and, in the statistical setting, only in a relaxed "Las Vegas" form where the evaluator may declare failure.

Category. *Information-Theoretic Cryptography.*

Conjecture (informal). *In an additive randomized encoding, each of k parties locally encodes its input as one element of an abelian group; the group sum of the encodings must reveal the value of a fixed function f on the inputs and nothing else. It is the algebraic heart of non-interactive secure computation in the shuffle model, since shuffling gives secure addition for free. The prevailing belief was that statistically secure such encodings do not exist even for equality on a small domain; the source refutes that belief and builds them for every finite function. Its encodings, however, are only statistically* correct*: with small probability the evaluator gets the wrong answer, or — in the sharper "Las Vegas" variant — announces failure. In the computational setting, perfect correctness is known. The source asks whether every function admits an additive randomized encoding that is at once statistically secure and perfectly correct.*

1 The setting

An additive randomized encoding (ARE) for a k-party function f, introduced by Halevi, Ishai, Kushilevitz and Rabin [HIKR23], lets each party i map its input x_i to $\hat{x}_i$ in an abelian group $\mathbb{G}$; the evaluator sees only $\hat{w} = \hat{x}_1 + \cdots + \hat{x}_k$, from which it should decode

$f(x_1, \ldots, x_k)$ and learn nothing else. Any f with an ARE can be securely computed non-interactively in the shuffle model, because shuffling suffices for secure addition [IKOS06].

The feasibility landscape splits by how accurately the sum encoding must be simulatable. With *computational* security, every efficient function has an ARE, under a Diffie–Hellman-type assumption in bilinear groups [HIKR23], later reduced to any public-key encryption scheme [BEG25]. With *perfect* security, AREs exist only for degenerate functions — essentially OR and XOR with local pre- and post-processing [HIKR23, Hiw25]. The statistical middle was the open case, and the expectation ran the other way: the authors of [HIKR23] conjectured that statistical AREs do not exist even for equality over a small domain, a conjecture implied by the (still open) conjecture that shuffle privacy is weaker than central privacy.

The source refutes that conjecture. Its Theorem 1.1 states that for any multi-party $f : D^k \to D$ over a finite domain and any $\varepsilon > 0$ there is an ARE for f with statistical correctness and security errors at most ε; its Theorem 1.2 relates ARE size to garbling size, yielding efficient statistical AREs for NL/poly, and computational ones for P/poly from any one-way function with black-box use only.

What its constructions do not give is perfect correctness. The source records, in its "Open Questions": "*Perfect correctness.* Does every f admit a perfectly correct and statistically secure ARE? For computationally secure ARE, perfect correctness is possible [HIKR23, BEG25]. For ARE with statistical security, we are only able to achieve a relaxed *Las Vegas* notion of correctness, where the evaluator is never wrong but may declare failure with a small probability (see Appendix A)." So the gap is narrow and precisely located: the failure probability, not a wrong answer, is what is left to remove.

2 Notation and parameters

- k is the number of parties; $f : (\{0,1\}^n)^k \to \{0,1\}^m$ the function; D a finite domain where the source states $f : D^k \to D$.
- $(\mathbb{G}, +)$ is a finite abelian group, assumed *efficient*: representation size $c \log |\mathbb{G}|$ and operations in time $|\mathbb{G}|^c$ for a universal constant c.
- ε is the correctness error and δ the security error, both statis-

tical.

- $\Delta(X,Y)$ is statistical distance and $X \approx_\delta Y$ means $\Delta(X,Y) \le \delta$.
- Where an ARE is viewed as a family, τ is the security parameter and all costs, including group operations, are polynomial in τ.

3 The conjecture

Definition 1 (Additive randomized encoding, [BEGI25, Definition 2.1], after [HIKR23]). Let $f : (\{0,1\}^n)^k \to \{0,1\}^m$ be a k-party function. An ARE for f over an abelian group $(\mathbb{G},+)$ is a pair $\Pi = (\mathsf{Enc},\mathsf{Dec})$ where $\hat{x}_i \leftarrow \mathsf{Enc}(x_i,i) \in \mathbb{G}$ is randomized and $w \leftarrow \mathsf{Dec}(\hat{w})$ is deterministic, satisfying

- *ε-correctness*: for all $x_1,\dots,x_k \in \{0,1\}^n$,

$$\Pr\left[\mathsf{Dec}\left(\sum_{i=1}^k \mathsf{Enc}(x_i,i)\right) = f(x_1,\dots,x_k)\right] \ge 1-\varepsilon;$$

- *δ-security*: there is a simulator Sim with $\sum_{i=1}^k \mathsf{Enc}(x_i,i) \approx_\delta \mathsf{Sim}(f(x_1,\dots,x_k))$ for all $x_1,\dots,x_k \in \{0,1\}^n$.

The ARE is *perfectly correct* if it is 0-correct.

Conjecture 1 (Perfect correctness with statistical security). *For every k, every finite domain D, every k-party function $f : D^k \to D$ and every $\delta > 0$ there is an efficient abelian group $\mathbb{G}$ and an ARE for f over $\mathbb{G}$ (Definition 1) that is perfectly correct ($\varepsilon = 0$) and δ-secure.*

Remark 1 (Both directions are open, and the source picks neither). The source poses this as a question, not as a prediction. A resolution is either a construction as in Conjecture 1 or a proof that some finite f — equality over a small domain being the natural candidate, since it is the function the earlier conjecture [HIKR23] singled out — admits no perfectly correct δ-secure ARE for small enough δ. Note that the negative direction is not excluded by the source's Theorem 1.1: that theorem gives statistical correctness, and the whole content of this statement is whether the correctness error can be driven to exactly zero.

Remark 2 (Las Vegas correctness is what is already known). The source's Appendix A achieves a relaxation in which the decoder outputs either $f(x)$ or a distinguished failure symbol, never a wrong value, with failure probability at most ε. Under Definition 1 that is a ε-correct ARE and not a perfectly correct one, and Conjecture 1 is not settled by it. A construction whose decoder may output $\perp$ therefore does not resolve this statement, however small the failure probability.

Remark 3 (Efficiency is not part of the question). Conjecture 1 is a feasibility statement over finite domains, matching the source's Theorem 1.1, and imposes no bound on the ARE's size beyond the group being efficient in the sense of Section 2. The source's separate size question — how close the ARE size of f can come to its garbling size, and whether efficient information-theoretic AREs extend from NL/poly to all of P/poly, which it notes would settle a long-standing open problem of [FKN94] — is a different statement.

Remark 4 (Two other open questions in the same list). The source's "Open Questions" section also asks whether information-theoretic feasibility extends to the *robust* ARE notion of [HIKR23] for finite functions — where a positive answer even for finite 3-party functions would settle the main open question on multi-party randomized encodings [ABT21], and for all finite functions the main open question on best-possible information-theoretic MPC [HIKR18] — and whether a 2-party PSM protocol for f on n-bit inputs implies an ARE for f of similar cost. Neither is this statement.

4 Bibliography

[BEGI25] Nir Bitansky, Saroja Erabelli, Rachit Garg and Yuval Ishai. *Shuffling is universal: statistical additive randomized encodings for all functions.* IACR ePrint 2025/1442. The source. Definition 2.1 is on page 7, Theorem 1.1 on page 2, and the open question is the first item of Section 1.4 ("Open Questions"), page 7.

[HIKR23] Shai Halevi, Yuval Ishai, Eyal Kushilevitz and Tal Rabin. *Additive randomized encodings and their applications.* CRYPTO 2023, Part I, LNCS 14081. Introduces ARE and robust ARE, gives the computational construction from bilinear groups, and conjectures statistical AREs do not exist — the conjecture the source refutes.

[BEG25] Nir Bitansky, Saroja Erabelli and Rachit Garg. *Additive randomized encodings from public key encryption.* IACR ePrint 2025/104, to appear in CRYPTO 2025. Reduces computational ARE to any public-key encryption scheme, with perfect correctness.

[Hiw25] Keitaro Hiwatashi. *Negative results on information-theoretic additive randomized encodings.* Applied Cryptography and Network Security (ACNS), 2025, pages 136–157. Characterizes which Boolean functions admit AREs with security and correctness measured in the ℓ_2 norm; cited by the source alongside [HIKR23] for the perfect-security impossibility.

[ABT21] Benny Applebaum, Zvika Brakerski and Rotem Tsabary. *Perfect secure computation in two rounds.* SIAM Journal on Computing, 50(1):68–97, 2021. The multi-party randomized encoding question a robust-ARE feasibility result would settle.

[HIKR18] Shai Halevi, Yuval Ishai, Eyal Kushilevitz and Tal Rabin. *Best possible information-theoretic MPC.* TCC 2018, Part II, LNCS 11240, pages 255–281. The best-possible-MPC question a robust-ARE feasibility result for all finite functions would settle.

[IKOS06] Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky and Amit Sahai. *Cryptography from anonymity.* 47th Annual IEEE Symposium on Foundations of Computer Science (FOCS), 2006, pages 239–248. Shuffling suffices for secure addition, which is what links ARE to the shuffle model.

[FKN94] Uriel Feige, Joe Kilian and Moni Naor. *A minimal model for secure computation.* 26th Annual ACM Symposium on Theory of Computing (STOC), 1994, pages 554–563. Introduces private simultaneous messages; the long-standing open problem the source's efficiency question would settle.