CONJURA · OPEN PROBLEM

Malicious NISC with Constant Communication Overhead from a Black-Box PRG

Random bit-OT correlations, no random oracle

Status. Statement: AI-written from Yuval Ishai, Ziyang Jin, Naty Peter and Akshayaram Srinivasan, *Non-Interactive Secure Computation with Constant Communication Overhead*, IACR ePrint 2026/1555. Not yet checked by a human. The source poses this question and then answers the variant in which the pseudorandom generator is replaced by a random oracle, which leaves the question as posed — black-box PRG, no idealized primitive — unresolved.

Category. *Secure Multiparty Computation.*

Conjecture (informal). *Non-interactive secure computation is Yao's protocol at its most rigid: the receiver sends one message, the sender replies once, and that is the whole interaction. With semi-honest parties, random OT correlations and a pseudorandom generator, the cost is $O(|C|\lambda)$ bits — a constant factor over the circuit size times the security parameter, and about the best one can hope for without homomorphic machinery. Against malicious parties, every route to that same constant factor has needed something extra: more rounds, or a weaker "correlated abort" security notion, or OLE-style correlations far more expensive to generate than OT, or a random oracle. The source asks whether the extra ingredient can be dispensed with entirely — constant overhead, malicious security, one round each way, from OT correlations and black-box use of a PRG — and then proves the version of its own question in which the PRG is replaced by a random oracle.*

1 The setting

In the semi-honest setting a NISC protocol for a Boolean circuit C costs $O(|C|\lambda)$ bits of communication, given a setup of random bit-OT correlations and a PRG, and the source notes that without homomorphic primitives such as fully homomorphic encryption or homomorphic secret sharing this is the best one could hope

for barring a major breakthrough. The malicious setting has been messier. Ishai et al. [IKO+11] achieved a polylog$(|C|,\sigma)$ multiplicative overhead with black-box use of a PRG; Afshar et al. [AMPR14] achieved overhead σ, asymptotically worse but concretely better at realistic σ; Hazay et al. [HIV17] achieved constant overhead in the random oracle model, but with either extra rounds or the weaker "correlated abort" notion, in which the sender can force the receiver to abort depending on a sender-chosen predicate of the receiver's input; and Dittmer et al. [DILO22] achieved constant overhead with standard security but from programmable OLE correlations, which are considerably more expensive to generate than OT correlations [BCG+19].

The source states the resulting question in a display of its own: "Is there a malicious-secure NISC protocol with communication cost $O(|C|\lambda)$ assuming random OT correlations and black-box use of PRG?", adding that such a protocol "would bridge the asymptotic gap between what is known in a semi-honest setting and what is known in a malicious setting".

Its own answer changes one hypothesis. "For the question above, we show that if we replace a PRG by a random oracle, we can indeed close the above gap": its Theorem 1.1 gives a malicious-secure two-party NISC protocol for any Boolean circuit C with communication $O(|C|\lambda)$, assuming random bit-OT correlations and a random oracle, with standard (not correlated-abort) security. The random oracle is used substantively — to instantiate the IPS watchlist by Fiat–Shamir, following [IKSS22a], and inside the commitments of the Ligero-style sublinear proof its inner protocol depends on — so the question as posed, with a PRG used only as a black box and no idealized primitive, is what remains.

2 Notation and parameters

- C is a Boolean circuit computing the two-party function; $|C|$ is its number of gates.
- λ is an exact computational security parameter, σ a statistical security parameter allowing $2^{-\sigma}$ simulation error.
- *Random OT correlations* means random bit-OT correlations: the receiver holds (b, s_b) and the sender (s_0, s_1) for uniform bits, one instance per unit of setup.

- *Black-box use of a PRG* means the protocol invokes a pseudorandom generator as an oracle and its security reduces to the PRG's, with no use of the PRG's code.
- Communication cost counts all bits sent in the two messages, excluding the correlated-randomness setup.

3 The conjecture

Definition 1 (NISC with malicious security). A *non-interactive secure computation* protocol for a two-party function f consists of one message from the receiver to the sender and one message back, both parties additionally holding a setup of random bit-OT correlations sampled independently of their inputs. It is *malicious-secure* if for every efficient adversary corrupting either party there is an efficient simulator such that the real and ideal executions are computationally indistinguishable, in the standard (not correlated-abort) sense: a corrupted sender's ability to make the receiver abort must not depend on the receiver's input.

Conjecture 1 (Constant overhead from a black-box PRG). *There is a malicious-secure NISC protocol (Definition 1) for every Boolean circuit C with communication cost $O(|C|\lambda)$ bits, assuming random bit-OT correlations and black-box use of a pseudorandom generator, and no idealized primitive.*

Remark 1 (What the source's own theorem does and does not settle). The source's Theorem 1.1 establishes Conjecture 1 with "black-box use of a pseudorandom generator" replaced by "a random oracle". That is a strengthening of the assumption, not a weakening, so Conjecture 1 is untouched by it; equally, the source's result means a resolution has to beat a known protocol rather than build the first one, and the plausible route is to de-idealize that protocol rather than to start over. Two uses of the oracle would have to go: the Fiat–Shamir instantiation of the watchlist, and the commitments in the Ligero-style sublinear proof system used to keep the inner protocol's proofs short.

Remark 2 (Every relaxation is already known). Conjecture 1 is

tight against the literature in four directions at once, and dropping any one of them makes it a known result: allow polylog$(|C|,\sigma)$ overhead and it is [IKO+11]; allow correlated-abort security and it is [IKO+11, HIV17] (in the random oracle model); allow more rounds and it is one of the constant-round protocols with constant overhead [HIV17]; allow programmable OLE correlations in place of OT and it is [DILO22]. A resolution therefore has to hold all four fixed.

Remark 3 (Direction, and what a negative answer would look like). The source phrases this as a question and expresses no expectation; it merely notes that a positive answer would bridge the semi-honest and malicious asymptotics. A negative answer would be a lower bound of an unusual kind — separating black-box PRG use from random-oracle use at a fixed communication budget, in a fixed round pattern, with a fixed setup — and no such separation is claimed or hinted at in the source.

4 Bibliography

[IJPS26] Yuval Ishai, Ziyang Jin, Naty Peter and Akshayaram Srinivasan. *Non-interactive secure computation with constant communication overhead.* IACR ePrint 2026/1555. The source. The question is displayed on page 2; Theorem 1.1 and the sentence resolving the random-oracle variant are on page 3; Table 1 comparing prior work is on page 3.

[IKO+11] Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, Manoj Prabhakaran and Amit Sahai. *Efficient non-interactive secure computation.* EUROCRYPT 2011, LNCS 6632, pages 406–425. The first malicious-secure NISC with black-box use of cryptography, achieving polylog$(|C|,\sigma)$ multiplicative overhead from OT correlations and a PRG, and implicitly a constant-overhead protocol with correlated abort.

[IPS08] Yuval Ishai, Manoj Prabhakaran and Amit Sahai. *Founding cryptography on oblivious transfer — efficiently.* CRYPTO 2008, LNCS 5157, pages 572–591. The compiler — outer protocol, inner protocol, watchlist — the source's construction builds on.

[AMPR14] Arash Afshar, Payman Mohassel, Benny Pinkas and Ben Riva. *Non-interactive secure computation based on cut-and-choose.* EUROCRYPT 2014, LNCS 8441, pages 387–404. Malicious NISC with multiplicative overhead σ, concretely better than the polylogarithmic-overhead protocol at realistic σ.

[HIV17] Carmit Hazay, Yuval Ishai and Muthuramakrishnan Venkitasubramaniam. *Actively secure garbled circuits with constant communication overhead in the plain model.* TCC 2017, Part II, LNCS 10678, pages 3–39. Constant-overhead constant-round protocols in the random oracle model, either with extra rounds or with correlated-abort security.

[DILO22] Samuel Dittmer, Yuval Ishai, Steve Lu and Rafail Ostrovsky. *Authenticated garbling from simple correlations.* CRYPTO 2022, Part IV, LNCS 13510, pages 57–87. Malicious NISC with constant overhead from programmable OLE correlations.

[BCG+19] Elette Boyle, Geoffroy Couteau, Niv Gilboa, Yuval Ishai, Lisa Kohl and Peter Scholl. *Efficient pseudorandom correlation generators: silent OT extension and more.* CRYPTO 2019, Part III, LNCS 11694, pages 489–518. Cited by the source for the cost of generating OLE-style correlations relative to OT correlations.

[IKSS22a] Yuval Ishai, Dakshita Khurana, Amit Sahai and Akshayaram Srinivasan. *Round-optimal black-box protocol compilers.* EUROCRYPT 2022, Part I, LNCS 13275, pages 210–240. Weakens the watchlist requirement so that it can be instantiated in the random oracle model by Fiat–Shamir.

[AHIV17] Scott Ames, Carmit Hazay, Yuval Ishai and Muthuramakrishnan Venkitasubramaniam. *Ligero: lightweight sublinear arguments without a trusted setup.* ACM CCS 2017, pages 2087–2104. The proof system whose interleaved Reed–Solomon test the source's inner protocol uses, and whose commitments are one of the two places the random oracle enters.