Limits of Random Oracles in Secure Computation

Background

Impagliazzo-Rudich [3] showed that a Random Oracle is not sufficient to implement public-key encryption information-theoretically, thereby establishing a fundamental qualitative separation between public-key and private-key cryptography. This also had implications for Secure Function Evaluation or SFE (wherein Alice and Bob with inputs x and y, resp., compute f(x,y) without revealing further information): Oblivious Transfer and other "complete" functions cannot be implemented using only a Random Oracle.

Our Results

We show that an RO, by itself (without computational assumptions), is useful for secure function evaluation exactly as much as an ideal commitment functionality is: f can be securely computed in the RO-model iff it can be computed in the "commitment-hybrid" model.

In particular, for security against semi-honest (passive) adversaries, an RO is not useful at all.

This holds for all 2-party deterministic SFE functions (even unsymmetric ones) with polynomial-domains.

What Does It Tell Us?

Informally, the computational hardness needed for secure evaluation of any function that does not have an unconditionally secure protocol, is more complex than what one-way functions (or any other "mini-crypt") primitive that can be implemented in the RO-model provide. This can be formalized as the impossibility of a "fully blackbox reduction" [5] of SFE to one-way functions.

These are the first results since [2], separating secure computation from mini-crypt primitives.

Future Work

Our result is specific to deterministic SFE, as our analysis uses their combinatorial structure. No such structure is known for randomized SFE. But if we can "compile" the RO in any secure protocol, our result can be extended to randomized SFE as well.

In ongoing work, Bob oracles other than RO, that can lead to separations of SFE from public-key encryptions as well. More generally, we ask if we can uncover many works in "Impagliazzo’s universe" for various (qualitatively different) SFE functionalities.

Preliminaries

1. Decomposable and Undecomposable Functions:

Decomposable functions are exactly those for which there are 2-party SFE protocols [3]. There are many undecomposable functions that are not complete. These are the ones for which our characterization newly rules SFE protocols in the RO model.

2. Protocol Tree for a 2-party protocol: Has an (Alice) and B (Bob) nodes, that represent partial transcripts, with an edge from an A-node (resp. B-node) u to v if the next message from Alice (resp. Bob) given transcript u results in transcript v. The weight on an edge is the probability P[v|x,u,y] where x,y are inputs.

3. Frontier Analysis of Protocols: We shall consider "frontiers" on the protocol tree where for the first time some property holds. For example [4] used frontiers (k = 1) where for the first time some significant amount of additional information about x (resp. y) is revealed by a single message.

4. Independence Learner: Following [2], there exists an Learner who queries the RO polynomially many times at each round, so that a locality property holds conditioned on Expert view so far. Alice’s next message is almost independent of Bob’s input (and vice-versa).

5. Augmented Protocol Tree: Contains Alice, Bob and Eve nodes. On an edge coming out of an Eve-node, Eve’s interaction with RO is added to the transcript.

Proof Intuition

Suppose an undecomposable function f has a semi-honest SFE protocol in the RO model.

Plan: Define frontier Fx in the augmented protocol tree where a significant amount of new information about x is revealed by Alice, or is accumulated since last message from Alice. Similarly, Fy. Then:

Fx and Fy are almost "full": a transcript should pass through both, except with small probability. Fx occurs on a random transcript path) "at or above" F1 only with small probability; similarly for Fy occurring "at or above" F2.

Together we get a contradiction.

- Completeness: because some information about both inputs must always be revealed (because of correctness and security, and undecomposability).
- Fx is not strictly above F1 (and similarly, Fy is not strictly above F2) with significant probability: Else, Alice is revealing information about x independent of y, can be shown to be insecure, f is undecomposable.
- But could Fx and Fy coincide?

Intuitively, locality property ⇒ child of an A-node not on F1, and child of a B-node not on F2.

- But Fx & Fy could coincide at children of Eve-nodes.

Then information first revealed could be Eve, could depend on both x and y, and even be f(x,y) itself.

To rule out this we give an attack to show that in case Eve’s oracle queries reveal some information about x and y, then one of the two parties can extract (non-ideal) information using an imaginary execution (with a simulated RO) in which it alters its input.

Some Technical Details

Apared relation: If a node v is the child of an A-node, then A[ordered] = Parent(v) else, if v is the last node that is a child of an A-node on the path from root to v. (See fig.)

Similarly Bpared is defined.

For (suitably chosen δ and δ): the distributions are based on protocol execution with a random oracle and random inputs.

Similarly, F1 is defined in terms of Bpared.


Suppose not. Then:

- Relying on undecomposability, we identify a suitable 2×2 minor of inputs (x,y)→(y,y), so that f(x,y)≠f(x,y) but f(y,y)=f(y,y), and ∃ G of size x≥y, s.t. P[EE|x,y, G] > (1+δ)P[EE|x,y, G] where ee=A[ordered], and A[ordered] occurs strictly above F1, and P[EE|x,y, G] is large.

We contradict this:

- Let G = x+y ∈ R. s.t. piped(G) are Alice nodes, and A[ordered] are children of Alice nodes.

(F1) can be bounded using the locality property.

- We bound P(I|x,y) by giving an attack at Rx.

Attack at the Frontier

1. Rx is the part of the frontier Fx such that for v ∈ Rx, v = A[ordered] is the child of an Alice node, v occurs strictly above F1, and P[EE|x,y, G] > (1+δ)P[EE|x,y, G].

Claim: P[R|x,y] is small.

If not how we show a curious Bob with input y’ can mentally switch to y and distinguish between x and x’.

On reaching u Bob samples an alternate view Vx(u) corresponding input y. He simulates a RO condition on this view and Alice’s input x (which he doesn’t know) using access to the actual RO (which is conditioned on x and Vx(u)’s : queries in blue and orange views are answered according to those views; queries in green region are both answered, and the other queries are answered using the actual RO. This works because of a "safety property" of the independence learner: that (w.h.p.) the orange and green regions don’t intersect the gray region.

References


Research supported by NSF grants CNS-0707207, CNS-0716522, CNS-0704699, APStAR Award FA9550-10-1-0093, DAPR and an AFRL contract F18806-11-1-0201. This submission has not been previously published and the views of these agencies.

Mohammad Mahmoody
Cornell University
Hemanta K. Maji
University of California Los Angeles
Manoj Prabhakaran
University of Illinois Urbana-Champaign