## Background

Secure function evaluation is one of the most widely studied problems in secure multiparty computation. Coin-tossing is among basic cryptographic primitives that have been well-studied.

It is known that with computational assumption, coin-tossings are complete, i.e., the most complex and powerful.

However, surprisingly, there has been no systematic study of the power of coin-tossing in computationally unbounded settings.

## Goals

Show that coin-tossing only has limited power to help realize other functionalities, that is
- Coin-tossing does not help realize any deterministic task
- Coin-tossing only helps realize randomized task in a trivial sense

## Fundamental Questions/Challenges

Do these results hold for more than two parties?

What about unsymmetric SFE functionalities?

## Technique Employed

We develop a new technique called the frontier analysis of protocols. This involves analyzing carefully defined frontiers in a weighted binary tree of the protocol.

## Research Results

There is no standalone secure protocol for XOR, another very basic functionality, even if we have an access to public coin-tossing.

The consequence is that deterministic functionality $f$ has a secure protocol in $F_{\text{coin}}$ hybrid world if and only if $f$ has a secure protocol in the plain model (UC or standalone).

We also show that coin-tossing helps very little in realizing randomized functionality. Intuitively, functionalities have secure realization in $F_{\text{coin}}$ hybrid world if and only if they have the form of first evaluating a deterministic functionality and then obtaining some trusted coins.