Towards practical verifiable computation: verification outsourcing, linear arguments without linearity tests, and repeated structures

Gang Xu

November 14, 2014

Abstract

Cloud Computing represents a new trend in modern computing. But while outsourcing computation provides appealing benefits, one must fully consider a critical security issue: there is no guarantee on the correctness of the results. Thus an immediate need for result assurance naturally arises. This need motivates a growing body of research on verification of outsourced computation. While state-of-the-art schemes are asymptotically efficient, the constants on their running times are large, and they seem too intricate to be implemented easily. This dissertation focuses on the verifiable computation, taking steps towards bringing it closer to practicality.

We argue that since the verification may be tedious and expensive, users are likely to outsource (again) the verification workload to a third party. Other scenarios such as auditing and arbitrating may also require the use of third-party verification. Outsourcing verification will introduce new security challenges. One such challenge is to protect the computational task and the results from the untrusted third party verifier. In this work, we address this problem by proposing an efficient verification outsourcing scheme. To our knowledge, this is the first solution to the verification outsourcing problem. We show that, without using expensive fully-homomorphic encryption, an honest-but-curious third party can help to verify the result of an outsourced computational task without having to learn either the computational task or the result thereof.

Besides the introduction of the verification outsourcing paradigm, we also bring improvements to the state-of-the-art verification protocol designs. We firstly investigate the linearity tests, which overwhelmingly occupy the bandwidth of the interaction part of the state-of-the-art designs based on linear PCP. Our results show that under certain assumptions, the linearity tests in the combined linear PCP become redundant. Our theoretical result immediately results in RIVER, a new linear-PCP-based argument system which achieves lower cost. Then, we focus on the computations with repeated sub-structures and design a novel verification protocol, that takes advantage of these particular features. we notice loops play a pivotal role in the real world of computing (not only compute-intensive computations but also data-intensive computations such as big data applications). Thus, we take loops as a typical example and show that the circuit generated from computation with loops can indeed lead to a lower amortized cost and a lower cost of proof generation. Using the theory of arithmetic circuit complexity we prove that for most programs our design results in very significant savings.