Cryptology ePrint Archive: Report 2011/597

How to Delegate and Verify in Public: Verifiable Computation from Attribute-based Encryption

Bryan Parno and Mariana Raykova and Vinod Vaikuntanathan

Abstract: The wide variety of small, computationally weak devices, and the growing number of computationally intensive tasks makes the delegation of computation to large data centers a desirable solution. However, computation outsourcing is useful only when the returned result can be trusted, which makes verifiable computation (VC) a must for such scenarios. In this work we extend the definition of verifiable computation in two important directions: public delegation and public verifiability, which have important applications in many practical delegation scenarios. Yet, existing VC constructions based on standard cryptographic assumptions fail to achieve these properties.

As the primary contribution of our work, we establish an important (and somewhat surprising) connection between verifiable computation and attribute-based encryption (ABE), a primitive that has been widely studied. Namely, we show how to construct a VC scheme with public delegation and public verifiability from any ABE scheme. The VC scheme verifies any function in the class of functions covered by the permissible ABE policies. This scheme enjoys a very efficient verification algorithm that depends only on the output size. Strengthening this connection, we show a construction of a multi-function verifiable computation scheme from an ABE with outsourced decryption, a primitive defined recently by Green, Hohenberger and Waters (USENIX Security 2011). A multi-function VC scheme allows the verifiable evaluation of multiple functions on the same preprocessed input.

In the other direction, we also explore the construction of an ABE scheme from verifiable computation protocols.

Category / Keywords: cryptographic protocols / Verifiable, Computation, Delegation, Public-Key Cryptography, Attribute-Based Encryption

Date: received 3 Nov 2011

Contact author: parno at microsoft com