Cryptology ePrint Archive: Report 2011/337

Collusion Resistant Obfuscation and Functional Re-encryption

Nishanth Chandran and Melissa Chase and Vinod Vaikuntanathan

Abstract: Program Obfuscation is the problem of transforming a program into one which is functionally equivalent, yet whose inner workings are completely unintelligible to an adversary. Despite its immense cryptographic utility, program obfuscation has proved to be a hard and elusive goal, as evidenced by the wide-ranging impossibility results, starting with the work of Barak {\em et al.}~(CRYPTO 2001). There is a limited, although steadily increasing, set of positive results in this area, including obfuscation of point functions, proximity testing, testing of hyperplane membership, and obfuscating re-encryption programs.

The presence of auxiliary inputs about secrets is a practical and omnipresent concern in cryptography, and the case of program obfuscation is no different. Achieving program obfuscation was hard to begin with; achieving secure obfuscation in the presence of auxiliary information about the program is downright daunting. In particular, virtually no positive results are known in this setting.

In this work, we define a specific form of auxiliary input security, called \emph{collusion-resistant} obfuscation. Informally, we consider a setting where the program to be obfuscated is composed of many ``pieces'', each one chosen by a different party. The question then is: does the obfuscation remain secure, even if the adversary gets hold of the pieces of the program belonging to a subset of the parties? Thus, the auxiliary input here is simply the various pieces of the program.

Following the work of Hohenberger {\em et al.}~(TCC 2007), we consider the notion of average-case secure obfuscation and define collusion resistance with respect to this notion. We then show how to obfuscate a natural and complex cryptographic functionality called {\em functional re-encryption}. Informally, the functional re-encryption functionality for a public-key encryption scheme and a policy function F with n possible outputs is one that transforms (``re-encrypts'') an encryption of a message $m$ under an ``input public key'' into an encryption of the same message m under one of the n ``output public keys'', namely the public key indexed by $F(m)$. We show how to obfuscate functional re-encryption for any policy function F (with a polynomial-size domain) using bilinear maps.

In a nutshell, our result shows how to achieve a meaningful relaxation of the highly useful yet elusive notion of auxiliary input security, for a sophisticated cryptographic functionality.

Category / Keywords: public-key cryptography / re-encryption, obfuscation

Date: received 22 Jun 2011

Contact author: melissac at microsoft com