Research

Theoretical Computer Science Seminar

Symbolic Methods in the Formal Analysis of Automatically Synthesized Cryptographic Algorithms

Prof. Andrew Marshall
University of Mary Washington

06/11/2020
11:00 Horas

`link:`TBA

Abstract. While symbolic methods have long been applied to cryptographic protocol analysis, there has been comparatively little done on developing new classes of symbolic techniques specifically for application to automated synthesis of cryptographic algorithms. However, since the symbolic algebras used in the evaluation of automatically synthesized cryptosystems have much in common with those used in the analysis of cryptographic protocols, a promising direction in research is to build on these previously developed methods combined with new methods to make advances in the symbolic analysis of automatically synthesized cryptosystems.

Many of the symbolic characterizations are expressed in terms of the existence or non-existence of solutions to systems of equations. Thus, unification, the process of finding solutions to systems of equations in a symbolic algebra, is an important tool in this approach. However, the unification algorithms in this setting often need to obey certain constraints. For example, the solutions may need to be computable by a probabilistic polynomial-time adversary without access to certain terms (e.g. some cryptographic keys), or a solution may require that certain terms not be identical, thus adding a disunification constraint. Additionally, an authentication algorithm may require that authentication checks (which usually involve checking an inequality) succeed for correctly authenticated data and fail for all other cases. Thus, this area requires the development of new unification methods and algorithms.

In this talk we provide some background material to this symbolic approach to the analysis of these types of cryptographic systems. We then detail several new problems and results with a focus on new unification algorithms. We review a new tool for automating some of the above methods. Finally, we outline some future work and open questions.