Cryptology ePrint Archive: Report 2013/161

Completeness Theorems for All Finite Stateless 2-Party Primitives

Daniel Kraschewski

Abstract: Since Kilian showed in 1988 that oblivious transfer (OT) is complete in the sense that every secure multi-party computation can be realized from this primitive, cryptographers are working on reductions of OT to various other primitives. A long-standing open question in this context is the classification of finite stateless 2-party primitives (so-called "cryptogates"), i.e. trusted black boxes that can be jointly queried by two parties, have finite input and output alphabets, and do not change behavior depending on time or input history. Over the decades, completeness criteria have been found for deterministic cryptogates (i.e. primitives without internal randomness), noisy channels, and symmetric (i.e., both parties receive the same output) or asymmetric (i.e., only one party receives any output at all) randomized cryptogates. However, the known criteria for randomized primitives other than noisy channels only hold in presence of passive adversaries (i.e., even corrupted parties still follow the protocol).

We complete this line of research by providing simple but comprehensive combinatorial completeness criteria for ALL finite stateless 2-party primitives. I.e., for the first time there are completeness criteria for randomized primitives that are neither symmetric nor asymmetric (but give different outputs to the querying parties), and we overcome the limitation that previous results for randomized primitives with input from BOTH parties only regarded passive adversaries. A fundamental tool of our approach is a powerful lemma from real algebraic geometry, which allows us to base a cryptographic security proof on a rather "game-theoretic" approach.

As a corollary of our work, every non-complete example of a finite stateless 2-party primitive is essentially symmetric. This relationship between non-completeness and symmetric output behavior was previously only known for deterministic cryptogates.

Category / Keywords: foundations / oblivious transfer, complete primitives, information-theoretic security, universal composability, secure function evaluation

Date: received 19 Mar 2013, last revised 8 May 2013

Contact author: kraschewski at kit edu