Title: Overlaying Branches in Garbled Circuits

Vladimir Kolesnikov, Bell Labs, USA

We identify a promising direction in Garbled Circuit (GC) research and propose heuristics that improve GC for circuits with switch statements. Our techniques also improve semi-private function evaluation (SPF-SFE), whose goal is to hide from GC evaluator (privacy-critical) portions of the evaluated function.

An important drawback in the GC approach is the need to garble, send and evaluate the entire GC, even though often only a small portion of it needs to be evaluated. This is the case, e.g., when the program contains switch statements, and evaluates one of several branches based on a private input or an internal variable. We show how to greatly reduce this overhead. Our approach relies on two technical contributions. Combining them results in eliminating the need to transfer all the GC's branches.

First, we show how, given circuits C1, … ,Ck and viewing them as directed acyclic graphs (DAGs) D1, …, Dk, to embed them in a new graph D0. The embedding is such that a GC garbling of any of C1, …, Ck could be implemented by a corresponding garbling of a circuit corresponding to D0. The size of D0 is often much smaller than the sum of the sizes of D1, …, Dk.

Second, we show how, obliviously to both players, to cheaply generate, transmit and evaluate the garbling of D0, implementing the Ci being evaluated. (The standard approach would require sending all k garblings). In the practically important case when circuit generator knows the evaluated clause (such as SFP-SFE), a single garbling of D0 is sent, resulting in factor 3.6x improvement in our experiments.

This is joint work with Sean Kennedy and Gordon Wilfong (Bell Labs).