Büscher, Niklas; Franz, Martin; Holzer, Andreas; Veith, Helmut; Katzenbeisser, Stefan

On compiling Boolean circuits optimized for secure multi-party computation. (English)

Zbl 1386.68020


Summary: Secure multi-party computation (MPC) allows two or more distrusting parties to jointly evaluate a function over private inputs. For a long time considered to be a purely theoretical concept, MPC transitioned into a practical and powerful tool to build privacy-enhancing technologies. However, the practicality of MPC is hindered by the difficulty to implement applications on top of the underlying cryptographic protocols. This is because the manual construction of efficient applications, which need to be represented as Boolean or arithmetic circuits, is a complex, error-prone, and time-consuming task. To facilitate the development of further privacy-enhancing technology, multiple compilers have been proposed that create circuits for MPC. Yet, almost all presented compilers only support domain specific languages or provide very limited optimization methods. In this work we describe our compiler CBMC-GC that implements a complete tool chain from ANSI C to circuit. Moreover, we give a comprehensive overview of circuit minimization techniques, which we have identified and adapted for the creation of efficient circuits for MPC. With the help of these techniques, our compilation approach allows for a high level of abstraction from the cryptographic primitives used in MPC protocols, as well as the complex design of digital circuits. By using the model checker CBMC as a compiler frontend, we illustrate the link between MPC, formal methods, and digital logic design. Our experimental results illustrate the effectiveness of the implemented optimizations techniques for various example applications. In particular, compared with other state-of-the-art compilers, we show that CBMC-GC compiles circuits from the same source code that are up to four times smaller.

MSC:

68M14 Distributed systems
68N20 Theory of compilers and interpreters
68P25 Data encryption (aspects in computer science)
94C10 Switching theory, application of Boolean algebra; Boolean functions (MSC2010)

Keywords:
secure multi-party computation; compiler; logic synthesis

Software:
ABC; CBMC; JustGarble; TASTY; TinyGarble; ObliVM; Sharemind; Frigate; ABY; Obliv-C

Full Text: DOI

References:


This reference list is based on information provided by the publisher or from digital mathematics libraries. Its items are heuristically matched to zbMATH identifiers and may contain data conversion errors. It attempts to reflect the references listed in the original paper as accurately as possible without claiming the completeness or perfect precision of the matching.