Garbled Circuits mit signierten Eingaben

Hintergrund:

Sichere Mehrparteienberechnung beschäftigt sich damit, wie mehrere Parteien gemeinsam eine Funktion auf ihren privaten Eingaben berechnen können. Dabei soll gewährleistet sein, dass niemand mehr lernt, als er aus seiner Ein- und Ausgabe ableiten kann, und dass das Ergebnis korrekt berechnet wird.

Ein Ansatz für sichere Mehrparteienberechnung sind sogenannte „Garbled Circuits“[BeHR12], bei welchen die zu berechnende Funktion als Schaltkreis dargestellt wird, welcher dann von einer Partei (dem Garbler) so verschlüsselt wird, dass die andere Partei (der Evaluator) die Funktion auswerten kann, ohne die Eingaben des Garblers zu lernen.

Die beiden gängigen Sicherheitsmodelle sind dabei „semi-honest“, wobei Angreifer sich an das Protokoll halten und lediglich versuchen, mehr Informationen als vorgesehen zu lernen, und „malicious“, wobei Angreifer beliebig vom Protokoll abweichen können um sowohl mehr Informationen zu lernen als auch das Ergebnis zu verändern.
Außer acht gelassen wird hierbei jedoch, ob Parteien die „richtigen“ Eingaben verwenden:
In vielen Szenarien kann es sinnvoll sein, dass eine vertrauenswürdige Partei Eingaben signiert, und nur solche Eingaben erwünscht sind, welche über eine Signatur verfügen.

Aufgabenstellung:

Ausgangspunkt ist das Papier „Enforcing Input Correctness via Certification in Garbled Circuit Evaluation“ von Zhang, Blanton und Bayatbabolghani [ZhBB17], welches ein Verfahren beschreibt, bei welchem sichergestellt wird, dass der Garbler signierte Eingaben verwendet.

In einem ersten Schritt soll der skizzenhafte Sicherheitsbeweis in [ZhBB17] formal ausgearbeitet werden.

Anschließend soll das Verfahren so angepasst/erweitert werden, dass es die „Free XOR“[KoSc08] Verbesserung unterstützt.

Betreuer: Markus Raiber, markus.raiber@kit.edu

[BeHR12] BELLARE, MIHIR ; HOANG, VIET TUNG ; ROGAWAY, PHILLIP: Foundations of Garbled Circuits. In: *Proceedings of the 2012 ACM Conference on Computer and Communications Security, CCS ’12*. New York, NY, USA : ACM, 2012. — event-place: Raleigh, North Carolina, USA — ISBN 978-1-4503-1651-4, S. 784–796

[KoSc08] KOLESNIKOV, VLADIMIR ; SCHNEIDER, THOMAS: Improved Garbled Circuit: Free XOR Gates and Applications. In: ACETO, L. ; DAMGÅRD, I. ; GOLDBERG, L. A. ; HALLDÓRSSON, M. M. ; INGÓLFSDÓTTIR, A. ; WALUKIEWICZ, I. (Hrsg.): *Automata, Languages and Programming, Lecture Notes in Computer Science* : Springer Berlin Heidelberg, 2008 — ISBN 978-3-540-70583-3, S. 486–498

[ZhBB17] ZHANG, YIHUA ; BLANTON, MARINA ; BAYATBABOLGHANI, FATTANEH: Enforcing Input Correctness via Certification in Garbled Circuit Evaluation. In: FOLEY, S. N. ; GOLLMANN, D. ; SNEKKENES, E. (Hrsg.): *Computer Security – ESORICS 2017, Lecture Notes in Computer Science*. Cham : Springer International Publishing, 2017 — ISBN 978-3-319-66399-9, S. 552–569