Karlsruhe Institute of Technology

Institut für Theoretische Informatik
Lehrstuhl Prof. Dr. J. Müller-Quade
crypto.iti.kit.edu

Praxis der Forschung Wintersemester 2019/20 + Sommersemester 2020

Lattice-based black-box accumulation

Untersuchung der Möglichkeit die kryptographischen Bausteine aus BBA auf anzunehmend post-quantum sichere Annahmen zu basieren. Als hoffentlich post-quantum sichere Annahme wir eine Gitterannahme ausgewählt.

Black-box accumulation (BBA) wurde als Baustein für eine Vielzahl kundenorientierte Protokolle wie Loyalitäts-, Pfand-, und Bonussysteme. Vereinfacht gesprochen kann man diesen Baustein als „Sparschwein“ sehen, welches Benutzer erlaubt Punkte (oder dergleichen) zu sammeln und zwar in einer anonymen und unverknüpfbaren Art und Weise.

Explizit sollen zu Beginn die verwendeteten kryptographischen Bausteine aus BBA herausgearbeitet werden. Anschließend wird untersucht ob es für diese schon gitterbasierte Primitiven gibt. Falls nicht, wird die Möglichkeit der Übertragung auf Gitterannahmen überprüft – in rein theoretischer Form und/oder in angewandter Form für BBA. Danach wird überprüft ob die gitterbasierte Primitive noch effizient genug ist – in rein theoretischer Form und/oder in implemtierter Form. Des Weiteren wird geschaut, welche Sicherheit von BBA mit den gitterbasierten kryptographischen Bausteinen gewährleistet werden kann.

Voraussetzungen:

- Vorkenntnisse im Bereich der Kryptographie sind vorteilhaft, können aber auch während der Arbeit erarbeitet werden
- Interesse an der Problemstellung und Eigeninitiative sind ausdrücklich erwünscht ☺

Bei Interesse oder Fragen zur Aufgabenstellung freue ich mich über eine kurze E-Mail.

Betreuer:
Astrid Ottenhues: Zi. 251 (Geb. 50.34), astrid.ottenhues@kit.edu
Alexander Koch: Zi. 274 (Geb. 50.34), alexander.koch@kit.edu