Karlsruher Institut für Technologie

Institut für Theoretische Informatik (ITI)
Kryptographie und Sicherheit
Prof. Dr. Jörn Müller-Quade

Deck- und kartenminimale spielkartenbasierte sichere Mehrparteienberechnung

Projektgruppe „Praxis der Forschung“
Wintersemester 2017/18

1 Themenbeschreibung

Kryptographie ist weit mehr als nur Verschlüsselung. Mit der sogenannten sicheren Mehrparteienberechnung können verschiedene Akteure gemeinsam eine Funktion berechnen, ohne dabei etwas über die privaten Eingaben der jeweils anderen zu lernen (das nicht bereits durch die Ausgabe offensichtlich ist). So können z. B. zwei Spieler durch Berechnung eines logischen UNDs bestimmen, ob gegenseitiges romantisches Interesse besteht, ohne dass bei nur einseitigem Interesse die Gefahr besteht, dass die jeweils andere Person dies erfährt.

Im Bereich der „Spielkartenbasierten Kryptographie“ braucht man hierfür nur ein paar Spielkarten mit ununterscheidbarer Rückseite – es geht also gänzlich ohne Computer. Neben dem Schutz vor Trojanern, die einfach die Eingabe mitlesen, sind diese kryptographischen Protokolle vor allem für die Demonstration von sicherer Mehrparteienberechnung in didaktischen Kontexten interessant. Ein Ziel ist es, solche Protokolle zu entwerfen, die möglichst wenig Karten verwenden und z. B. durch die geeignete/eingeschränkte Wahl der Mischoperationen auf den Karten einfach durchführbar sind.

Der Großteil der Literatur verwendet Decks die auf den Vorderseiten nur die Symbole Herz (♥) und Kreuz (♣) haben. Wir möchten stattdessen Protokolle entwerfen, die z. B. ein einziges Standard-Spielkarten-Deck mit sämtlich unterscheidbaren Symbolen $1, \ldots, 52$ verwenden, oder untere Schranken für die Anzahl von Karten in UND-Protokollen in diesem Setting beweisen. Je nach Einschränkung an die Mischoperation sind hierfür auch Vorkenntnisse im Bereich der Gruppentheorie (Gruppenaktionen, Orbit, Stabilisator, etc.) hilfreich.

2 Kapazitäten

Bei guten Teamplayern ist auch eine Gruppe aus zwei oder drei Teilnehmern möglich.

3 Kontakt / Betreuer

Alexander Koch alexander.koch@kit.edu, Raum 274 (Geb. 50.34)