Über idealisierte Berechnungsmodelle in der Kryptologie

Tibor Jager

Das *Generische Gruppen Modell* (GGM) betrachtet Algorithmen, die Berechnungen auf Elementen aus einer algebraischen Gruppe ausführen, ohne dabei die konkrete Darstellung der Gruppenelemente (zum Beispiel als ganze Zahlen oder Punkte auf einer elliptischen Kurve) auszunutzen. Dies wird modelliert, indem man die Gruppe als *Black-Box* betrachtet. Ein Algorithmus kann mit dieser Black-Box interagieren, um zum Beispiel Berechnungen oder Gleichheitstests durchzuführen.

Algorithmen, die ein gegebenes Berechnungsproblem im GGM lösen, sind unabhängig von der konkreten Darstellung der Gruppenelemente. Daher nennt man sie *generisch*. Wichtige Beispiele aus der Kryptologie sind Pollard's Rho oder der Baby-Step Giant-Step Algorithmus zur Berechnung diskreter Logarithmen.

Generische Gruppen und ihre Erweiterungen zu generischen bilinearen Gruppen und generischen Ringen werden in der Kryptologie als Werkzeuge benutzt, um klassische und neue Komplexitätsannahmen zu analysieren. Es gibt jedoch zahlreiche grundlegende Fragen, die noch unbeantwortet sind.

- Sind diese Modelle in der Form, wie sie derzeit in der kryptographischen Literatur eingesetzt werden, eine vernünftige Abstraktion der Realität?
- Können wir die Modelle näher an die Realität bringen? Die Herausforderung dabei ist, die Modelle so realistisch wie möglich zu machen, es aber trotzdem zu ermöglichen Aussagen zu beweisen, die (noch) nicht im Standardmodell beweisbar sind.
- Eines der wichtigsten offenen Probleme in der Kryptologie ist die Frage, ob das Diffie-Hellman Problem äquivalent zum diskreten Logarithmusproblem ist. Eine *generische* Reduktion wäre besonders interessant, da dies die Äquivalenz beider Probleme in *allen* Gruppen implizieren würde. Gibt es eine solche Reduktion?

Die Dissertation leistet Beiträge zur Beantwortung dieser Fragen:

- Es wird gezeigt, dass das Generische Ring Modell (GRM), wie es derzeit in der Literatur benutzt wird, die Realität nur unzureichend modelliert: Es gibt *natürliche* Berechnungsprobleme, welche im GRM beweisbar schwer sind, in der Realität jedoch leicht lösbar. Dies ist eine wichtige Beobachtung, um bekannte Ergebnisse im GRM interpretieren zu können.
- Es wird eine Variante des Generische Gruppen Modells vorgestellt. Dieses Modell umfasst erstmalig *alle bekannten Algorithmen* für kryptologisch relevante Berechnungsprobleme. Daher kann es wesentlich stärkere Aussagen über Komplexitätsannahmen treffen als das klassische GGM. Es wird auch die Nutzbarkeit des neuen Modells für die Analyse kryptographischer Komplexitätsannahmen demonstriert.
- Es wird gezeigt, dass eine effiziente generische Reduktion vom diskreten Logarithmusproblem auf das Diffie-Hellman Problem einen effizienten Faktorisierungsalgorithmus für ganze Zahlen impliziert. Unter der Annahme, dass Faktorisieren schwer ist, kann es eine solche Reduktion also nicht geben. Selbst wenn die Faktorisierungsannahme falsch ist, bedeutet es dass es sehr schwer ist eine generische Reduktion zu finden, da man dazu ein seit Jahrhunderten ungelöstes Problem lösen müsste.