Über die Möglichkeit und Unmöglichkeit scharfer Reduktionen in der Kryptographie

Christoph Bader

Bei der Entwicklung neuer kryptographischer Verfahren wird heutzutage neben der Konstruktionsvorschrift besonderer Wert auf den Sicherheitsbeweis gelegt. Oft wird der Beweis unter einer Komplexitätsannahme, die besagt, dass ein bestimmtes Problem schwer zu berechnen ist, gegeben. In diesem Fall beschreibt der Sicherheitsbeweis einen effizienten Algorithmus, die Reduktion, der einen erfolgreichen Angreifer gegen das neu entwickelte Verfahren effizient in einen weiteren Algorithmus, den Inverter, der das Berechnungsproblem löst, transformiert. Unter der Annahme, dass es keinen Algorithmus gibt, der das Berechnungsproblem effizient löst, kann es nun keinen effizienten Angreifer gegen das Verfahren geben: Falls es einen effizienten Angreifer gäbe, könnte man das Problem effizient lösen. Die Reduktion reduziert also das Brechen des schweren Problems auf das Brechen des neu entwickelten Verfahrens.

Die Qualität einer Reduktion kann bestimmt werden, indem man den Arbeitsaufwand (die erwartete Laufzeit) des Inverters mit dem Arbeitsaufwand des Angreifers vergleicht. Das Verhältnis von beiden wird *Verlust* der Reduktion genannt. Idealerweise ist der Arbeitsaufwand des Inverters nahezu identisch mit dem Arbeitsaufwand des Angreifers. In diesem Fall nennt man die Reduktion *scharf*.

Im Allgemeinen beeinflusst der Verlust einer Reduktion die Größe der Parameter, die verwendet werden, wenn ein kryptographisches Verfahren in der Praxis eingesetzt wird: Je kleiner der Verlust der Reduktion, desto kleiner die Parameter. Daher sind scharfe Reduktionen ein wünschtenswertes Ziel mit praktischen Anwendungen. Aus theoretischer Sicht sind scharfe Reduktionen evtl. noch interessanter, denn die Konstruktion von Verfahren, für die eine scharfe Reduktion möglich sind, verlangt neue Design-Ideen und Beweistechniken, welche die Fach-Gemeinschaft bereichern.

Gegenstand dieser Dissertation sind scharfe Sicherheitsbeweise für kryptographische Verfahren. Wir analysieren welche Voraussetzungen einen scharfen Sicherheitsbeweise unmöglich machen (unter bestimmten Komplexitätsannahmen). Andererseits geben wir Verfahren an, die scharfe Sicherheitsbeweise haben. Unser Unmöglichkeitsergebnis greift für die entwickelten Verfahren nicht, da diese nicht die erforderlichen Voraussetzungen erfüllen.