Geheimnisse sichern mit Mathematik

Björn und Sören Christensen

Wir leben in einer Welt, in der Informationen immer wichtiger werden, und gleichzeitig immer mehr Bedrohungen für deren Sicherheit existieren. So kennt jeder die Meldungen über Cyberangriffe auf Unternehmen oder das Veröffentlichen geheimer Regierungsinformationen durch Einzelne, wie vor Kurzem in den USA. Der Schutz von Daten ist also eine der wesentlichen Fragen unserer Zeit. Und wie in so vielen Bereichen handelt es sich auch hier oft um im Kern mathematische Fragen.

Dies nehmen wir zum Anlass, in dieser Woche ein Verfahren vorzustellen, das als „Shamir's Secret Sharing" (Shamirs Geheimnisteilung) bekannt ist, benannt nach seinem Erfinder Adi Shamir, einem israelischen Professor für Informatik. Um das Verfahren anschaulich zu erklären, stellen wir uns vor, dass in einem großen Tresor ein wichtiges Geheimnis liegt, etwa das geheime Rezept von Coca Cola oder der Plan für die militärische Verteidigung eines Landes im Angriffsfall.

Als Code ist eine Geradengleichung hinterlegt

Von Zeit zu Zeit muss eine Gruppe von Mitarbeitern auf dieses Geheimnis zugreifen, sodass alle einen Zugangscode erhalten. Um allerdings Missbrauch zu verhindern, möchte man, dass immer zwei Mitarbeiter nötig sind, um den Tresor zu öffnen. Die Schwierigkeit dabei ist, dass keiner allein den Tresor öffnen können soll, das Verfahren aber jeweils zweien den Zugang ermöglichen soll.

Adi Shamir hatte dazu eine einfache Idee, die Sie alle aus dem Mathematikunterricht kennen: Der Tresor lässt sich öffnen, indem man eine bestimmte Geradengleichung als Code hinterlegt. Die Mitarbeiter bekommen aber nicht direkt diese Geradengleichung, sondern jeder erhält einen Punkt, der auf der Geraden liegt. Durch jeden einzelnen Punkt gehen noch unendlich viele Geraden, sodass kein einzelner den Tresor öffnen kann.

Zwei Punkte zusammen legen eine Gerade aber schon eindeutig fest, sodass zwei Mitarbeiter ausreichen, um an das Geheimnis zu kommen. Auf diese Weise kann man mehrere Personen mit Einzelpunkten auf der Geraden ausstatten, sodass zwei – egal in welcher Zusammensetzung – den Zugangscode erfüllen können.

Diese Methode lässt sich noch verallgemeinern. Wenn man etwa wünscht, dass drei Mitarbeiter nötig sind, dann nimmt man anstelle von Geraden Parabeln, denn quadratische Funktionen sind durch drei Punkte festgelegt. Basierend auf elementarer Mathematik lässt sich so also die Sicherheit von geheimen Informationen deutlich erhöhen.

Björn Christensen ist Professor für Statistik und Mathematik an der FH Kiel. **Sören Christensen** ist Professor für Stochastik an der Christian-Albrechts-Universität Kiel.