Sichere verteilte Daten und private Berechnungen

Die moderne Kryptographie beschäftigt sich nicht nur mit der Aufgabe, einen sicheren und geheimen Datenaustausch zwischen zwei Personen zu gewährleisten, sondern auch mit dem Problem, Daten sicher zu speichern, d.h. so auf einer Festplatte abzulegen, dass keiner, der keine Zugangsberechtigung hat, sie lesen kann. Eine zusätzliche Schwierigkeit ergibt sich, wenn diese Daten zudem nicht nur an einer Stelle, sondern auf vielen Rechnern gespeichert werden sollen.

Verteilte Geheimnisse

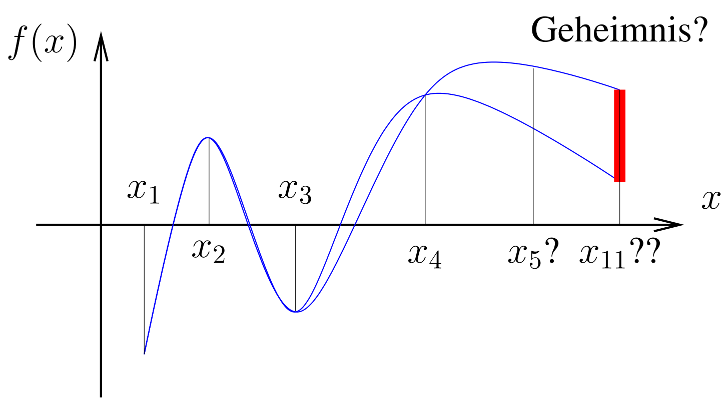
Die Aufgabenstellung der *verteilte Geheimnisse* kann durch folgendes Szenario beschrieben werden:

> Zehn Personen kaufen sich gemeinsam einen Film, der ihnen als Datei zugesendet wird. Jetzt möchten diese Personen verhindern, dass sich einzelne den Film alleine ansehen können, bevor sich das erste Mal mindestens fünf von ihnen zusammen gefunden haben.

Eine mögliche Lösungsstrategie für dieses Problem beruht auf der Analyse von Polynomen. Es ist bekannt, dass ein Polynom der Form

$$f(x) \;=\; a_4 \cdot x^4 \;+\; a_3 \cdot x^3 \;+\; a_2 \cdot x^2 \;+\; a_1 \cdot x \;+\; a_0$$

durch fünf Wertepaare $(x, f(x))$ eindeutig bestimmt ist — mehr als fünf schaden jedoch nicht. Geben wir also jedem der zehn Personen ein Wertepaar $(x_i, f(x_i))$,so können sie $f(x_{11})$ für einen bestimmten Wert x_{11} nur dann berechnen, wenn sich mindestens fünf von ihnen treffen. Mit Hilfe dieser Idee können wir das oben beschriebene Problem lösen.



Private Berechnungen

Eine mit der oben betrachteten Aufgabe verwandte Fragestellung sind so genannte *privaten Berechnungen*. Jeder Teilnehmer eine Gruppe kennt ein Geheimnis, das er natürlich nicht verraten möchte. Wir möchten jedoch eine Aufgabe lösen, die von allen Geheimnissen abhängigt. Betrachten wir folgendes Beispiel.

> Im Bundesrat steht eine wichtige Abstimmung über die Steuerreform auf dem Programm. Um den Fraktionszwang zu umgehen, soll diese Abstimmung absolut geheim stattfinden. Nach der Abstimmung soll nur bekannt sein, ob die Reform angenommen oder abgelehnt wurde. Selbst die genaue Anzahl der Ja- und Nein-Stimmen soll geheim bleiben. Um die Abstimmung durchzuführen, dürfen sich die Abgeordneten untereinander unterhalten.

Zur Lösung solcher Fragen gibt es zwei grundsätzliche Herangehensweisen. Die erste bedient sich kryptographischer Verfahren. Wir nennen diese Form der Berechnung auch kryptographisch private Berechnung. Diese Lösungsmethoden können jedoch nur so sicher sein wie die zugrunde liegenden Verschlüsselungsverfahren.

Die zweite Herangehensweisen versucht die Sicherheit der Geheimnisse mit Hilfe von Zufall und abhörsicheren Unterhaltungen zu lösen. Wir fordern bei dieser Form einer Berechnung, dass es für jeden Teilnehmer unmöglich sein muss (auch wenn er noch soviel Rechenkraft und Intelligenz benutzen kann), etwas über das Geheimnis irgendeines anderen zu erfahren. Um dies genauer zu erläutern, diskutieren wir ein weiteres Beispiel.

> 15 Jahre nach dem Abitur treffen sich Anton, Bärbel und Christine. Alle drei haben Karriere gemacht und wollen jetzt erfahren, wie hoch ihr Durchschnittseinkommen ist. Da jeder jedoch befürchtet, das kleinste Gehalt zu haben, wollen sie die Berechnung privat durchführen. Sie können sich jedoch schnell darauf einigen, dass sie in der Summe weniger als $1\,000\,000$ Euro im Monat verdient.

Dieses Problem können wir wie folgt lösen: Anton wählt zufällig eine Zahl r zwischen 0 und $999\,999$. Er addiert sein Einkommen hinzu und flüstert das Ergebnis Bärbel ins Ohr. Bärbel addiert ihr Einkommen und flüstert das Ergebnis Christine ins Ohr. Christine addiert ebenfalls ihr Einkommen. Das Ergebnis flüstert sie wiederum Anton ins Ohr. Dieser addiert $1\,000\,000 - r$ auf die erhaltene Zahl. Bei jeder der Additionen ist darauf zu achten, dass $1\,000\,000$ von der Summe abgezogen wird, falls diese größer oder gleich $1\,000\,000$ ist.

Was wurde berechnet? Wir bezeichnen mit a, b bzw. c das Einkommen von Anton, Bärbel bzw. Christine. Die Zahl, die Anton zum Schluss berechnet hat, ist der ganzzahlige Rest von $a + b + c + r + 1\,000\,000 - r$ bei Division durch $1\,000\,000$. Da wir wissen, dass $a+b+c < 1\,000\,000$ ist, ist dieser Rest gerade $a+b+c$. Also hat Anton die Summe der Einkommen berechnet, kennt also auch deren Durchschnitt.