Zero-Knowledge-Beweise

Das Modell der Zero-Knowledge-Beweise wurde 1985 von Goldreich, Micali und Rackoff entwickelt. Obwohl diese Form von Beweisen also noch sehr jung ist, ist eine Anwendung dieser Technik schon aus dem 16. Jahrhundert bekannt.

Tartaglias Lösung für Gleichungen dritten Grades

Um das Jahr 1535 fand der in Oberitalien lebende Niccolò Fontana (1499–1557; genannt „Tartaglia“, der Stammler) eine Formel, mit deren Hilfe sich viele Polynome dritten Grades, d.h. Gleichungen der Form $x^3 + a \cdot x^2 + b \cdot x + c = 0$ lösen lassen, nämlich solche mit $a = 0$. Obwohl diese Entdeckung ein bahnbrechendes Ereignis darstellte, wollte Tartaglia, der selber keinen akademischen Grad besaß, seine Lösungsformel geheimhalten.

Für positive Zahlen p, q ist

$$\sqrt[3]{\sqrt[2]{\left(\frac{p}{3}\right)^3 + \left(\frac{q}{3}\right)^2} + \frac{q}{3}} + \sqrt[3]{\sqrt[2]{\left(\frac{p}{3}\right)^3 + \left(\frac{q}{3}\right)^2} - \frac{q}{3}}$$

eine Lösung der Gleichung $x^3 + p \cdot x - q = 0$.

Um jedoch das Wissen über diese Lösung dem italienischen Rechenmeister Antonio Maria Fior zu beweisen, ohne sein Geheimnis zu verraten, benutzten die beiden folgendes Verfahren:

1. Fior wählte 30 Aufgaben der Form $x^3 + p \cdot x - q = 0$ und legte diese Tartaglia vor. Hierfür ist es lediglich nötig, für Zahlen r, s, t die Polynome $(y - r) \cdot (y - s) \cdot (y - t) = y^3 + a \cdot y^2 + b \cdot y + c$ zu bilden und y durch $x - \frac{a}{3}$ zu ersetzen. Die resultierende Formel hat oft die gewünschte Form.

2. Tartaglia berechnet die erste Nullstelle über die von ihm gefundenden Formel und die verbleibenden Nullstellen mit Hilfe der p, q-Formel. (Gleichungen der Form $x^2 + p \cdot x + q = 0$ haben die Lösungen $-\frac{p}{2} \pm \sqrt{\frac{p}{2}^2 - q}$.)

Betrachten wir nun die Eigenschaften dieses Protokolls:

1. Kennt Tartaglia die Lösungsformel, so kann er alle Fragen von Fior beantworten und Fior kann deren Korrektheit ohne Probleme verifizieren. Beantwortet Tartaglia alle Fragen korrekt, so kann sich Fior ziemlich sicher sein, dass Tartaglia ein Lösungsverfahren für solche Gleichungen kennt.

2. Fior erhält aus den Antworten von Tartaglia keine Information über das Lösungsverfahren. Auch ein Außenstehender hat keine Möglichkeit, etwas über die Lösungsformel zu erfahren.

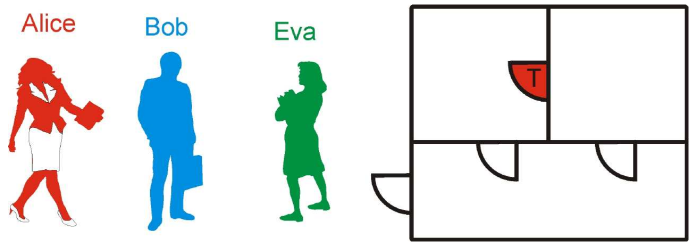
Diese Punkte stellen die wesentlichen Eigenschaften von Zero-Knowledge-Beweisen dar, die auch in der Kryptographie von großer Bedeutung sind. Betrachten wir ein Protokoll von drei Personen: Alice (die sich über ein geheimes Wissen identifizieren will), Bob (der die Aussage von Alice überprüfen möchte) und Eva (die die Unterhaltung belauscht, aber nichts erfahren soll):

1. Alice kann Bob von ihrem Wissen überzeugen,

2. Bob erfährt nur, dass Alice etwas weiß, aber nicht, was sie weiß, und

3. Eva erfährt nichts aus der Unterhaltung.

Ein Beispiel: Die magische Tür



In der Wohnung rechts kann die Tür T nur durch ein Passwort geöffnet werden. Alice behauptet, dass sie dieses Passwort kennt, aber sie will es nicht verraten. Bob möchte überprüfen, ob Alice tatsächlich das Passwort kennt. Obwohl Eva Bob auf Schritt und Tritt verfolgt, möchte Alice Bob von ihrem Wissen überzeugen, ohne dass Eva erfahren soll, ob Alice das Passwort tatsächlich kennt.

Es liegt also eine typische Situation für einen Zero-Knowledge-Beweis vor. Wie können wir dieses Problem lösen?

1. Bob wirft eine Münze. Damit bestimmt er, aus welchem Raum Alice in den Vorraum kommen soll. Das Ergebnis hält er vor Alice und Eva geheim. Anschließend gibt er entweder seine Entscheidung oder eine unbedeutende Notiz an Alice weiter. Dies wird wieder vor Eva geheim gehalten.

2. Alice betritt nun den Vorraum. Alle Türen werden verschlossen. Hat Bob Alice mitgeteilt, aus welchem Raum sie nachher herauskommen soll, dann geht sie in diesen Raum. Ansonsten wirft sie eine Münze, um sich für einen der beiden Räume zu entscheiden. Sie geht in diesen Raum und verschließt hinter sich die Tür.

3. Bob und Eva betreten den Vorraum. Bob sagt nun, aus welchem Raum Alice herauskommen soll. Kommt Alice aus dem richtigen Raum und hatte Bob im ersten Schritt Alice eine unbedeutende Nachricht gegeben, so ist das ein Hinweis für Bob, dass Alice das geheime Wort tatsächlich kennt. Da Eva jedoch nicht weiß, was auf der Nachricht von Bob an Alice stand, erfährt sie nichts.