Secret Sharing

15

In Public-Key-Infrastrukturen ist es oft nützlich, private Schlüssel von Teilnehmern rekonstruieren zu können. Wenn nämlich ein Benutzer die Chipkarte mit seinem geheimen Schlüssel verliert, kann er seine verschlüsselt gespeicherten Daten nicht mehr entschlüsseln. Aus Sicherheitsgründen ist es aber wichtig, dass nicht ein einzelner die Möglichkeit hat, geheime Schlüssel zu rekonstruieren. Es ist besser, wenn bei der Rekonstruktion von privaten Schlüsseln mehrere Personen zusammenarbeiten müssen. Die können sich dann gegenseitig kontrollieren. Die Wahrscheinlichkeit sinkt, dass Unberechtigte Zugang zu geheimen Schlüsseln bekommen. In diesem Kapitel wird eine Technik vorgestellt, dieses Problem zu lösen, das *Secret-Sharing*.

15.1 Prinzip

Wir beschreiben, was Secret-Sharing-Techniken leisten. Seien n und t natürliche Zahlen. In einem (n,t)-Secret-Sharing-Protokoll wird ein Geheimnis von einem *Dealer* auf n Personen aufgeteilt. Jeder hat einen Teil (Share) des Geheimnisses. Wenn sich t dieser Personen zusammentun, können sie das Geheimnis rekonstruieren. Wenn sich aber weniger als t dieser Geheimnisträger zusammentun, können sie keine relevante Information über das Geheimnis erhalten.

15.2 Das Shamir-Secret-Sharing-Protokoll

Seien $n,t \in \mathbb{N}$, $t \leq n$. Wir beschreiben das (n,t)-Secret-Sharing-Protokoll von Shamir [67]. Es verwendet eine Primzahl p und beruht auf folgendem Lemma.

J. Buchmann, *Einführung in die Kryptographie*, Springer-Lehrbuch,
DOI 10.1007/978-3-642-39775-2_15

Lemma 15.1 *Seien $\ell, t \in \mathbb{N}$, $\ell \leq t$. Weiter seien $x_i, y_i \in \mathbb{Z}/p\mathbb{Z}$, $1 \leq i \leq \ell$, wobei die x_i paarweise verschieden sind. Dann gibt es genau $p^{t-\ell}$* Polynome $b \in (\mathbb{Z}/p\mathbb{Z})[X]$ *vom Grad $\leq t-1$ mit $b(x_i) = y_i$, $1 \leq i \leq \ell$.*

Beweis Das Lagrange-Interpolationsverfahren liefert das Polynom

$$b(X) = \sum_{i=1}^{\ell} y_i \prod_{j=1, j\neq i}^{\ell} \frac{x_j - X}{x_j - x_i}, \tag{15.1}$$

das $b(x_i) = y_i$, $1 \leq i \leq \ell$ erfüllt. Jetzt muss noch die Anzahl solcher Polynome bestimmt werden.

Sei $b \in (\mathbb{Z}/p\mathbb{Z})[X]$ ein solches Polynom. Schreibe

$$b(X) = \sum_{j=0}^{t-1} b_j X^j, \quad b_j \in \mathbb{Z}/p\mathbb{Z}, 0 \leq j \leq t-1.$$

Aus $b(x_i) = y_i$, $1 \leq i \leq \ell$ erhält man das lineare Gleichungssystem

$$\begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{t-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{t-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_\ell & x_\ell^2 & \cdots & x_\ell^{t-1} \end{pmatrix} \begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{t-1} \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_\ell \end{pmatrix}. \tag{15.2}$$

Die Teil-Koeffizientenmatrix

$$U = \begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{\ell-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{\ell-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_\ell & x_\ell^2 & \cdots & x_\ell^{\ell-1} \end{pmatrix}$$

ist eine *Vandermonde-Matrix*. Ihre Determinante ist

$$\det U = \prod_{1 \leq i < j \leq \ell} (x_j - x_i).$$

Weil die x_i nach Voraussetzung paarweise verschieden sind, ist diese Determinante ungleich Null. Der Rang von U ist also ℓ. Daher hat der Kern der Koeffizientenmatrix des linearen Gleichungssystems (15.2) den Rang $t - \ell$ und die Anzahl der Lösungen ist $p^{t-\ell}$. □

Jetzt können wir das Protokoll beschreiben.

15.2.1 Initialisierung

Der Dealer wählt eine Primzahl p, $p \geq n+1$ und paarweise von Null verschiedene Elemente $x_i \in \mathbb{Z}/p\mathbb{Z}$, $1 \leq i \leq n$. Die Elemente von $\mathbb{Z}/p\mathbb{Z}$ werden zum Beispiel durch ihre kleinsten nicht negativen Vertreter dargestellt. Die x_i werden veröffentlicht.

15.2.2 Verteilung der Geheimnisteile

Der Dealer will ein Geheimnis $s \in \mathbb{Z}/p\mathbb{Z}$ verteilen.

1. Er wählt geheime Elemente $a_j \in \mathbb{Z}/p\mathbb{Z}$, $1 \leq j \leq t-1$ und konstruiert daraus das Polynom
$$a(X) = s + \sum_{j=1}^{t-1} a_j X^j. \tag{15.3}$$
Es ist vom Grad $\leq t-1$.
2. Der Dealer berechnet die Geheimnisteile $y_i = a(x_i)$, $1 \leq i \leq n$.
3. Der Dealer gibt dem i-ten Geheimnisträger den Geheimnisteil y_i, $1 \leq i \leq n$.

Das Geheimnis ist also der konstante Term $a(0)$ des Polynoms $a(X)$.

Beispiel 15.1 Sei $n = 5, t = 3$. Der Dealer wählt $p = 17$, $x_i = i$, $1 \leq i \leq 5$.

Das Geheimnis sei $s = 3$. Der Dealer wählt die geheimen Koeffizienten $a_i = 13 + i$, $1 \leq i \leq 2$. Damit ist also
$$a(X) = 15X^2 + 14X + 3. \tag{15.4}$$
Die Geheimnisteile sind damit $y_1 = a(1) = 15$, $y_2 = a(2) = 6$, $y_3 = a(3) = 10$, $y_4 = a(4) = 10$, $y_5 = a(5) = 6$.

15.2.3 Rekonstruktion des Geheimnisses

Angenommen, t Geheimnisträger arbeiten zusammen. Ihre Geheimnisteile seien $y_i = a(x_i)$, $1 \leq i \leq t$. Dabei ist $a(X)$ das Polynom aus (15.3). Dies kann man durch Umnummerierung der Geheimnisteile immer erreichen. Jetzt gilt
$$a(X) = \sum_{i=1}^{t} y_i \prod_{j=1, j\neq i}^{t} \frac{x_j - X}{x_j - x_i}. \tag{15.5}$$

Dieses Polynom erfüllt nämlich $a(x_i) = y_i$, $1 \leq i \leq t$ und nach Lemma 15.1 gibt es genau ein solches Polynom vom Grad höchstens $t-1$. Daher ist

$$s = a(0) = \sum_{i=1}^{t} y_i \prod_{j=1, j\neq i}^{t} \frac{x_j}{x_j - x_i}. \tag{15.6}$$

Die Formel (15.6) wird von den Geheimnisträgern benutzt, um das Geheimnis zu konstruieren.

Beispiel 15.2 Wir setzen das Beispiel 15.1 fort.

Die ersten drei Geheimnisträger rekonstruieren das Geheimnis. Die Lagrange-Interpolationsformel ergibt

$$a(0) = 15\frac{6}{2} + 6\frac{3}{-1} + 10\frac{2}{2} \bmod 17 = 3. \tag{15.7}$$

15.2.4 Sicherheit

Angenommen, weniger als t Geheimnisträger versuchen gemeinsam, das Geheimnis s zu ermitteln. Ihre Anzahl sei m, $m < t$. Ihre Geheimnisteile seien y_i, $1 \leq i \leq m$. Dies wird durch Umnummerierung der Geheimnisteile erreicht. Die Geheimnisträger wissen, dass das Geheimnis der konstante Term eines Polynoms $a \in \mathbb{Z}_p[X]$ vom Grad $\leq t-1$ ist, das $a(x_i) = y_i$, $1 \leq i \leq m$ erfüllt. Aus Lemma 15.1 erhält man das folgende Resultat.

Lemma 15.2 *Für jedes $s' \in \mathbb{Z}/p\mathbb{Z}$ gibt es genau p^{t-m-1} Polynome $a'(X) \in (\mathbb{Z}/p\mathbb{Z})[X]$ vom Grad $\leq t-1$ mit $a'(0) = s'$ und $a'(x_i) = y_i$, $1 \leq i \leq m$.*

Beweis Da die x_i paarweise und von Null verschieden sind, folgt die Behauptung aus Lemma 15.1 mit $\ell = m+1$. □

Lemma 15.2 zeigt, dass die m Geheimnisträger keine Information über das Geheimnis bekommen, weil alle möglichen konstanten Terme gleich wahrscheinlich sind.

15.3 Übungen

Übung 15.1 Rekonstruieren Sie das Geheimnis in Beispiel 15.1 aus den letzten drei Geheimnisteilen.

Übung 15.2 Sei $n = 4$, $t = 2$, $p = 11$, $s = 3$, $a_1 = 2$. Konstruieren Sie $a(X)$ und die Geheimnisteile y_i, $1 \leq i \leq 4$.