Secret Sharing

Das Teilen von Geheimnissen

Stefan Kluge

20.01.2017

Motivation

- Schutz wichtiger Systeme vor unberechtigtem Zugriff, z.B.
  - Schatzkarte
  - Datenbanken
  - Atomwaffen
- Wie können Geheimnisse vor Verlust bzw. Missbrauch geschützt werden
- Schlüssel an einer vermeintlich sicheren Stelle birgt Risiken, wie
  - Tod bei menschlichem Gehirn
  - technischen Defekt bei Festplatten
  - Diebstahl/Sabotage bei Tresor

Lösung: Secret Sharing

Lösung: das Geheimnis aufteilen

Das Geheimnis wird unter mehreren Parteien aufgeteilt. Dabei wird festgelegt, welche Parteien gemeinsam Zugriff auf das Geheimnis haben sollen und welche nicht.

Schwellenwertverfahren

Definition: (k, n)-Schwellenwertverfahren

Ein Verfahren zum Teilen von Geheimnissen wird (k, n)-*Schwellenwertverfahren* genannt, wenn es ein Geheimnis derart auf n Parteien verteilt, dass

- k oder mehr Parteien das Geheimnis gemeinsam rekonstruieren können
- $k - 1$ oder weniger Parteien das Geheimnis nicht rekonstruieren können.

Ein Verfahren wird *perfekt* genannt, wenn $k - 1$ oder weniger Personen aus ihren Teilgeheimnissen keine Information über das Geheimnis ableiten können.

Die ersten Lösungen

- erste Lösungen 1979 unabhängig voneinander entwickelt
- von George Blakley
  - basiert auf Schnitten von Hyperebenen in k-dimensionalen Räumen
- von Adi Shamir (das „S“ in RSA)
  - basiert auf Polynominterpolation über endlichen Körpern

Secret Sharing nach Shamir

Die Idee: Polynominterpolation

Sei $\mathbb{K}$ ein (endlicher) Körper. Dann gibt es zu k Punkten $(x_1, y_1), \ldots, (x_k, y_k) \in \mathbb{K}^2$ mit unterschiedlichen x_i ein eindeutig bestimmtes Polynom $p(x)$ vom Grad $k-1$ mit $p(x_i) = y_i$ für alle i.

Das Geheimnis wird zerlegt

Die Zutaten:

Seien $\mathbb{K}$ ein endlicher Körper und $G \in \mathbb{K}$ ein Geheimnis.

Der Geber wählt zufällig $a_1, a_2, \ldots, a_{k-1} \in \mathbb{K}$ und konstruiert damit das Polynom vom Grad $k-1$

$$p(x) = G + a_1 x + a_2 x^2 + \ldots + a_{k-1} x^{k-1}.$$

Anschließend wählt er n paarweise verschiedene Stellen $x_i \in \mathbb{K} \setminus \{0\}$ und errechnet daraus die Teilgeheimnisse

$$T_i = p(x_i) \qquad \text{für alle } 1 \leq i \leq n$$

Jede Partei P_i erhält als Teilgeheimnis das Paar (x_i, T_i).

Lagrange-Interpolation

Seien $(x_1, y_1), \ldots, (x_k, y_k)$ Punkte an unterschiedlichen Stellen. Dann haben die Lagrange-Basispolynome

$$\ell_i(x) = \prod_{\substack{j=1 \\ j \neq i}}^{k} \frac{x - x_j}{x_i - x_j}$$

die Eigenschaft $\ell_i(x_j) = \delta_{ij}$ und das Polynom

$$p(x) = \sum_{i=1}^{k} y_i \cdot \ell_i(x)$$

ist das eindeutig bestimmte Polynom mit $p(x_i) = y_i$ für alle $1 \leq i \leq k$,

k oder mehr Teilgeheimnisträger

Legen k oder mehr Parteien ihre Teilgeheimnisse zusammen, so können sie über Lagrange-Interpolation das Polynom $p(x)$ bestimmen. Das Geheimnis erhalten sie dann über

$$G = p(0) = \sum_{i=1}^{k} y_i \cdot \prod_{\substack{j=1 \\ j \neq i}}^{k} \frac{-x_j}{x_i - x_j}$$

Somit erfüllt das Secret Sharing nach Shamir die erste Bedingung an ein (k, n)-Schwellenwertverfahren.

$k-1$ oder weniger Parteien Teilgeheimnisträger

Nehmen wir an, jemand hat sich genau $k-1$ Teilgeheimnisse $(x_1, y_1), \ldots, (x_{k-1}, y_{k-1})$ verschafft. Dann gibt es zu jedem $G \in \mathbb{K}$ genau ein Polynom vom Grad $k-1$ mit

$$p(0) = G \qquad \text{und} \qquad p(x_i) = y_i \text{ für alle } 1 \leq i \leq k-1$$

Damit erfüllt Secret Sharing nach Shamir auch die zweite Bedingung für ein (k, n)-Schwellenwertverfahren.

Geheimnisse langfristig sicher halten

- Über die Zeit können Angreifer in den Besitz von einigen Teilgeheimnissen gelangen
- Lösung: Teilgeheimnisse in gewissen Abständen erneuern
- Der Geber erzeugt für das Geheimnis 0 ein zufälliges Polynom und die zugehörigen Teilgeheimnisse $T_1', T_2,', \ldots, T_n'$
- die Parteien addieren die $y-$ Werte ihrer Teilgeheimnisse und erhalten so ein neues Teilgeheimnis
- Die Eigenschaften bleiben wegen der Linearität erhalten

unehrliche Parteien

- Das Verfahren von Shamir ist sicher, solange sich die Parteien passiv verhalten
- Der Geber kann ungültige Teilgeheimnisse verteilen
- Die Parteien können versuchen mit gefälschten Teilgeheimnissen an Informationen zu gelangen
- Abhilfe schafft Verifiable Secret Sharing
- Dabei werden zusätzliche Informationen mitverteilt, mit denen die Gültigkeit der Teilgeheimnisse überprüft werden kann

Zugriffsstrukturen

Definition: Zugriffstruktur

Seien $M := \{P_1, P_2, \ldots, P_n\}$ eine Menge von Parteien. Eine Menge $\Gamma \subseteq \mathcal{P}(M)$ wird als Zugriffsstruktur bezeichnet, wenn für alle $B \in M$ folgende Bedingungen erfüllt sind

- Die Personengruppen B aus Γ sind die berechtigten Gruppen. Sie können gemeinsam das Geheimnis aus ihren Teilgeheimnissen ermitteln.
- Die Personengruppen $F \in \mathcal{P}(M) \setminus \Gamma$ sind nicht berechtigte Gruppen und können aus ihren Teilgeheimnissen nichts über das Geheimnis erfahren.

Das Verfahren von Shamir realisiert die Zugriffsstruktur

$$\Gamma = \{B \subseteq \mathcal{P}(M) | \#B \geq k\}$$

Quellen & Literatur I

- A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, 1979.
- D. R. Stinson, "An explication of secret sharing schemes," *Des. Codes Cryptography*, vol. 2, no. 4, pp. 357–390, 1992.
- A. Beimel, "Secret-sharing schemes: A survey," in *Coding and Cryptology - Third International Workshop, IWCC 2011, Qingdao, China, May 30-June 3, 2011. Proceedings*, pp. 11–46, 2011.
- P. Feldman, "A practical scheme for non-interactive verifiable secret sharing," in *28th Annual Symposium on Foundations of Computer Science, Los Angeles, California, USA, 27-29 October 1987*, pp. 427–437, 1987.

Quellen & Literatur II

A. Herzberg, S. Jarecki, H. Krawczyk, and M. Yung, "Proactive secret sharing or: How to cope with perpetual leakage," in *Advances in Cryptology - CRYPTO '95, 15th Annual International Cryptology Conference, Santa Barbara, California, USA, August 27-31, 1995, Proceedings*, pp. 339–352, 1995.