Seminar Kryptologie
Threshold Secret Sharing

Mirko Roth
TU-Braunschweig

20.Oktober 2003

1 Überblick

In dieser Ausarbeitung werden threshold secret sharing schemes (Schwellwert Schemata) behandelt. Dazu wird eine kurze Einführung in das Secret-Sharing gegeben. Im Speziellen werden weiterhin einzelne Schwellwert Schemata vorgestellt und erläutert wie z.B. das Shamir Schema.

2 Secret Sharing

Was ist Secret Sharing?

Das Problem des Secret-Sharing wurde 1979 von Adi Shamir aufgeworfen.
In diesem geht es um die Verteilung einer geheimen Information auf mehrere Teilnehmer, die diese Information später gemeinsam wieder rekonstruieren können. Im gleichen Jahr stellte Shamir ein Verfahren zur Lösung des Problems vor, welches in einem späteren Abschnitt erläutert wird.

Wo findet es seine Anwendung?

Es gibt Geheimnisse die „zu geheim“ sind um sie nur einer Person anzuvertrauen. Daher teilt man diese lieber auf mehrere Personen auf. Als Beispiel wären da die berühmten alten Piratenschatzkarten zu nennen. Diese wurden meisst vom Kapitän auf mehrere Mitglieder seiner Crew aufgeteilt, damit sie die erbeuteten Schätze nur gemeinsam wiederfinden können.
Weiterhin ist Secret Sharing auch eine Möglichkeit Geheimnisse vor Verlust zu schützen. Backups von Geheimnissen erhöhen deren Möglichkeit entdeckt und entschlüsselt zu werden. Möchte man aber trotzdem eine Kopie eines Geheimnisses erstellen, kann man diese mit Hilfe eines Secret-Sharing-Shemas auf mehrere Personen verteilen und somit vor Entdeckung schützen.
Kritische Aktionen beim Militär oder in Unternehmen bedürfen oft der Zustimmung mehrerer Personen. So ist z.B. das Öffnen eines bestimmten Kontos oder der Abschuss einer Rakete nur einem bestimmten Personenkreis vorbehalten. Dieser sollte dann auch nur gemeinsam in der Lage sein, eine solche Aktion durchzuführen. Auch hierfür eignet sich der Einsatz eines Secret-Sharing-Schemas.

Unter Secret Sharing versteht man also ein Verfahren, eine geheime Information *k* auf *n* Teilnehmer aufzuteilen, so das dieses Geheimnis *k* nur durch die Zusammenarbeit von hierfür qualifizierten Gruppen wiederhergestellt werden kann. Einzelne Teilnehmer oder nicht qualifizierte Gruppen von Teilnehmern sollen nicht in der Lage sein das Geheimnis zu rekonstruieren.

3 Threshold Secret Sharing

Ein (t, n) threshold secret sharing scheme (Schwellwert Schema) verteilt ein Geheimnis *k* auf mehrere Personen. Der Dealer verteilt das Geheimnis gleichmäßig auf *n* Personen. Diese Teilgeheimnisse werden Shares genannt, die Personen, Shareholder. Das Geheimnis wird so verteilt, das jede *t* oder mehr Anzahl von Shareholdern das Geheimnis wiederherstellen kann, wohingegen weniger als *t* Shareholder keine Information über das Geheimnis erlangen.
Die Wiederherstellung des Geheimnisses übernimmt der Combiner. Er ist erfolgreich, wenn die kooperierenden Shareholder mindestens *t* Mitglieder haben.

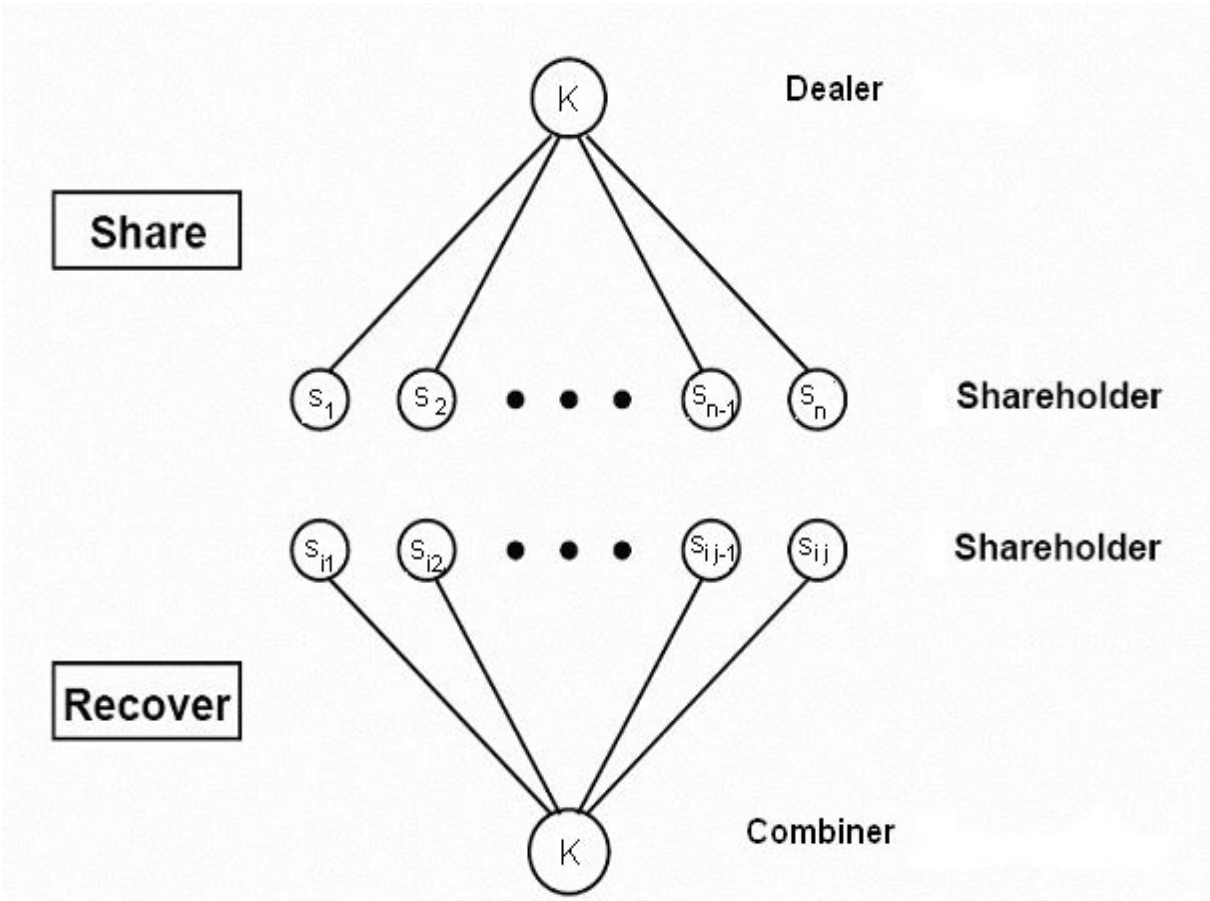

Abb. (*t, n) threshold secret sharing*

Weiterhin werden für die folgenden Protokolle und Schemata folgende Vereinbarungen getroffen.

- Der Dealer ist eine vertrauenswürdige Institution.
- Wir nehmen an, daß an den folgenden Schemata jeweils *n* Personen teilnehmen.
- Jedem Teilnehmer steht ein sicherer und geheimer Kommunikationsweg zur Verfügung.
- Die Shares gelangen auf diesen sicheren Kommunikationswegen zu den jeweiligen Shareholdern.
- Ein Schema wird als *perfekt* bezeichnet, wenn weniger als *t* Shareholder keine Information über das Geheimnis erlangen.

Definition: Ein (t,n) Schwellwert Schema (threshold scheme) besteht aus zwei aufeinanderfolgenden Algorithmen. Der erste Algorithmus der Dealer oder auch Share-Algorithmus

$$D: K \to S_1 \times S_2 \times ... \times S_n$$

verteilt die Teilgeheimnisse (Shares) des Geheimnisses $k \in K$ auf die Shareholder. Die Shares $s_i \in S_i$ werden über einen sicheren Kommunikationsweg an die jeweiligen Shareholder P_i übertragen.
Der zweite Algorithmus, der Combiner

$$C: S_{i_1} \times S_{i_2} \times ... \times S_{i_n}$$

versucht mit einer willkürlichen Anzahl von Shares das Geheimnis zu berechnen. Dem Algorithmus gelingt es nur dann das Geheimnis wiederherzustellen, wenn die Anzahl der Shares *i* größer oder gleich *t (i ≥ t)* ist. Ist die Anzahl der Shares *i* kleiner als *t* kann das Geheimnis nicht wiederhergestellt werden.

Ein (t, n) Schwellwert Schema ist *perfekt*, wenn jede Kombination von *(t-1)* Shares keine Information über das Geheimnis liefert.

4 (t, t) Schwellwert Schemata

Das Geheimnis eines (t, t) Schwellwert Schemas kann nur rekonstruiert werden, wenn alle Shareholder kooperieren. Eine einfache Implementierung ist z.B. folgende: Das Geheimnis $k \in Z_p$ wird so verteilt, das den *n* Teilnehmern jeweils zufällige Summanden zugeteilt werden, deren Summe dann wieder das Geheimnis ergibt. Der Dealer wählt ein zufälliges *p* mit *p > k*. Als nächstes wählt er zufällig *(t-1)* Elemente, s_1 , …, s_{t-1} aus Z_p .
Das Teilgeheimnis s_t ist: $s_t = k - \sum_{i=1}^{t-1} s_i (mod\ p)$.

Die Shares werden den Shareholdern $P=\{P_1,...,P_t\}$ auf sicheren Kommunikationswegen übermittelt. Der Combiner berechnet das Geheimnis mit Hilfe *aller* Shares wie folgt $k=\sum_{i=1}^{t} s_i (mod\ p)$.
Es ist zu ersehen das *(t-1)* und weniger Shares keine Information über das Geheimnis liefern. Das Verfahren ist also nach obiger Vereinbarung *perfekt*.
Das Verfahren hat aber einige Schwächen. Geht auch nur ein Teilgeheimnis verloren, kann das Geheimnis nicht wieder hergestellt werden. Weiterhin kann ein betrügerischer Shareholder durch Angabe eines falschen Shares das Ergebnis der Rekonstruktion verfälschen. Mit seinem Teilgeheimnis und dem falschen Ergebnis kann er dann das richtige Geheimnis leicht berechnen.
Dieses Verfahren wird aber dennoch verwendet, allerdings unter Verwendung von impliziten Geheimnissen zur annonymen Abstimmung mit notwendiger vollständiger Zustimmung aller Beteiligter. z.B. beim US Militär. Weiterhin finden (t,t) Schwellwert Schemata Anwendung bei der Konstruktion verschiedener Verfahren des General-Secret-Sharing.

5 Das Shamir Schema

Das 1979 von Shamir vorgestellte Schema ist ein (t,n) Schema und basiert auf Polynominterpolation. Alle Berechnungen werden im Ganzzahlkörper Z_p durchgeführt. Der Dealer Don wählt zunächst eine Primzahl *p* mit *p > k* und *p > n*. Weiterhin *n* verschiedenen Punkte $x_i \in Z_p$ für *i = 1,…,n*.
Danach bestimmt er ein beliebiges Polynom *P(x)* vom Grad *(t-1)* mit Koeffizienten a_i aus Z_p .

$$P(x)=a_0+a_1 x+...+a_{t-1}x^{t-1}\in Z_p$$

Die Shares sind $s_i=P(x_i)$ für *i = 1,..., n*. Das Geheimnis ist $k=P(0)$.

Wollen *t* oder mehr Shareholder das Geheimnis wiederherstellen versucht der Combiner Clara mit Hilfe der Shares das Polynom *P(x)* wiederherzustellen. Sie kennt *t* Punkte auf dem Polynom *P(x)*.

$$(x_{i_j}, f(x_{i_j}))=(x_{i_j}, s_{i_j}) \quad , j = 1,...,t\ .$$

Sie erhält also *t* (oder mehr) Gleichungen für *t* Unbekannte der Form

$$\begin{aligned} s_{i_1}&=a_0+a_1 x_{i_1}+...+a_{t-1}x_{i_1}^{t-1} \quad ,\\ s_{i_2}&=a_0+a_1 x_{i_2}+...+a_{t-1}x_{i_2}^{t-1} \quad ,\\ &\vdots\\ s_{i_t}&=a_0+a_1 x_{i_t}+...+a_{t-1}x_{i_t}^{t-1} \end{aligned}$$

Mit der zugehörigen Vandermonde-Determinante Δ .

$$\Delta = \begin{vmatrix} 1 & x_{i_1} & \dots & x_{i_1}^{t-1} \\ 1 & x_{i_2} & \dots & x_{i_2}^{t-1} \\ \dots & \dots & \dots & \dots \\ 1 & x_{i_t} & \dots & x_{i_t}^{t-1} \end{vmatrix} \neq 0$$

Dieses Gleichungssystem ist eindeutig lösbar und man erhält die Koeffizienten $a_0, \dots, a_{t-1}$ und damit auch das Geheimnis *k*.
Zur Bestimmung des Geheimnisses *k* ist die Ermittlung des ganzen Polynoms nicht notwendig. Mit Hilfe der Lagrange Interpolation lässt sich *k* aus *t* Punkten bei einem Polynom vom Grad *(t-1)* wie folgt berechnen

$$P(x) = \sum_{j=1}^{t} s_{i_j} \prod_{\substack{1 \le l \le t \\ l \neq j}} \frac{x - x_{i_l}}{x_{i_j} - x_{i_l}}$$

Für $k = P(0)$ ergibt sich dann:

$$k = a_0 = \sum_{j=1}^{t} s_{i_j} b_j \quad \text{mit} \quad b_j = \prod_{\substack{1 \le l \le t \\ l \neq j}} \frac{x_{i_l}}{x_{i_l} - x_{i_j}} \quad .$$

Erhält Clara nur *(t-1)* oder weniger Shares, entsteht ein Gleichungssystem mit *(t-1)* (oder weniger) Gleichungen und *t* Unbekannten. Dieses Gleichungssystem ist nicht eindeutig lösbar. Die Menge der Lösungen ergibt keine Information über das Geheimnis. Die Lösungen sind nicht von einem Zufallswert unterscheidbar. Damit ist das Shamir Schema nach obiger Vereinbarung perfekt.

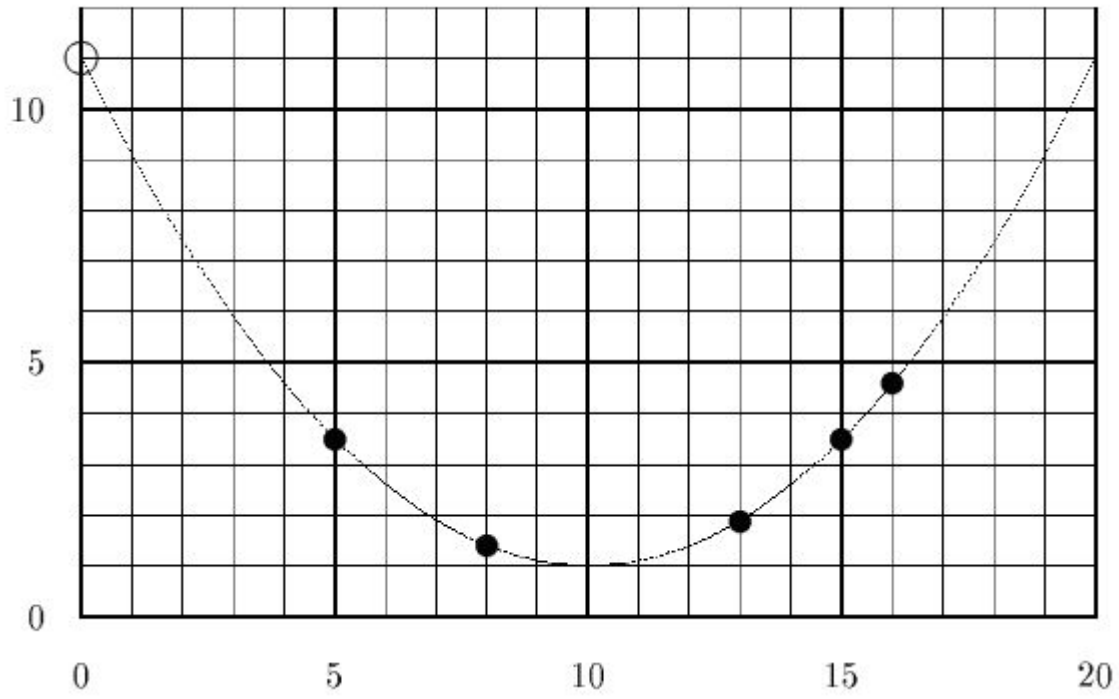

Abb. *(3,5) Schamir Schema*

Betrachten wir ein Beispiel eines (3, 6) Schamir Schemas über Z_7 .
Der Dealer wählt 6 Zahlen $x_i = i$ mit *i = 1,...,6*. Diese Werte auf der X-Achse sind öffentlich. Weiterhin bestimmt der Dealer mit dem Geheimnis *k=5* das Polynom $P(x) = 5 + 3x + 2x^2$. Die einzelnen Shares ergeben sich aus den Funktionswerten an den Stellen x_i . $s_1 = P(x_1) = P(1) = 3,\ s_2 = 5,\ s_3 = 4,\ s_4 = 0,\ s_5 = 0,\ s_6 = 4$.
Die Shares werden den jeweiligen Shareholdern übermittelt.

Die Shareholder P_1 , P_3 und P_6 entschliessen sich nun das Geheimnis zu rekonstruieren. Der Combiner erhält ihre Shares und somit folgende Punkte des Polynomes. *(1,3), (3,4) und (6,4),* (x_{i_j}, s_{i_j}) für *j=1...3* und das zugehörige Gleichungssystem:

$$\begin{aligned} 3 &= a_0 + a_1 + a_2 \\ 4 &= a_0 + 3a_1 + 2a_2 \\ 4 &= a_0 + 6a_1 + a_2 \end{aligned},$$

mit der Vandermonde-Determinante:

$$\Delta = \begin{vmatrix} 1 & 1 & 1 \\ 1 & 3 & 2 \\ 1 & 6 & 1 \end{vmatrix} = 2$$

Daher existiert eine eindeutige Lösung.

Mit $b_1 = 6,\ b_2 = 6,\ b_3 = 3$ ergibt sich für

$$k = a_0 = b_1 s_1 + b_2 s_3 + b_3 s_6 = 6 \cdot 3 + 6 \cdot 4 + 3 \cdot 4 = 54\ mod\ 7 = 5 \quad .$$

6 Das Blakley Schema

Blakley's ebenfalls im Jahre 1979 vorgestelltes Schwellwert Schema beruht auf geometrischer Konstruktion. Der Dealer Don wählt einen Vektorraum der Dimension *t* über dem Ganzzahlkörper Z_q . Don bestimmt einen Punkt *p* diesesVektor-raumes, der das Geheimnis darstellen soll.
Es existieren $\frac{(q^t - 1)}{(q - 1)}$ Untervektorräume der Dimension *(t-1)*. Ein Untervektorraum der Dimension *(t-1)* wird Hyperebene genannt. Shares sind nun verschiedene Hyperebenen des Vektorraumes welche den Punkt *p* enthalten.
Der Schnittpunkt aller Hyperebenen ist das Geheimnis.

Der Combiner Clara bestimmt den Schnittpunkt der Hyperebenen und somit das Geheimnis. Hat Clara nur *(t-1)* oder weniger Hyperebenen zur Verfügung, kann sie den Schnittpunkt nicht rekonstruieren.
Der Bereich in dem sich der Punkt befindet, lässt sich aber einschränken, da man die Information besitzt, das der Punkt *p* und somit das Geheimnis in der Schnitthyperebene liegt. Die Dimension der Hyperebene ist kleiner als die des

eigentlichen Vektorraumes. Somit gelangen *(t-1)* Shareholder an Informationen über das Geheimnis und das Blakley Schema ist nicht perfekt nach obiger Vereinbarung.

Beispiel für ein (2, 3) Blakley Schema.

Das Geheimnis ist der Punkt *(12,7)*. Zur Rekonstruktion des Geheimnisses sind mindestens 2 Geraden welche sich in diesem Punkt schneiden notwendig.
Wollen die Shareholder mit den Geraden $y=\frac{1}{2}x+1$ und $y=-x+19$ das Geheimnis rekonstruieren, berechnen sie den gemeinsamen Schnittpunkt ihrer Geraden. $-x+19=\frac{1}{2}x+1$ => $y=\frac{1}{2}x+1$ => *x=12, y=7*.

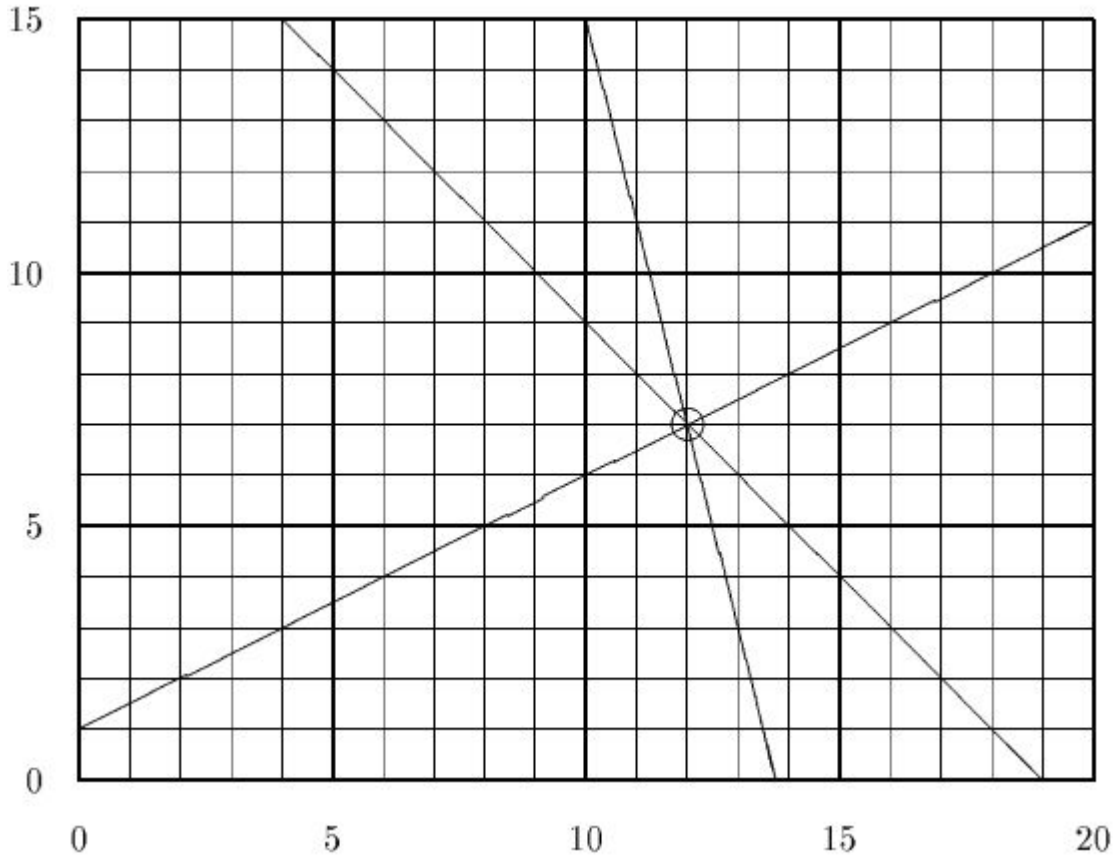

Abb. *(2,3) Blakley Schema in zwei Dimensionen*

7 Das Modular-Schema

Asmuth und Bloom benutzen in ihrem 1983 vorgestellten Verfahren Kongruenzen von Primzahlen um ein (t,n) Schwellwert Schema zu realisieren.
Der Dealer wählt öffentlich eine Primzahl p_0 . Jedem Teilnehmer $P_i \in P$ wird ein Modulus $p_i,\ i=1,\ldots,n$, zugeordnet. Dabei gilt $p_0 < p_1 < \ldots < p_n$. Die Moduli sind dabei Primzahlen.
Das Geheimnis *k* liegt in Z_{p_0} .

Der Dealer berechnet nun ein *s* für $k \equiv s (mod\ p_0)$ im Bereich $0 < s < \prod_{i=1}^{t} p_i$.

Dies ist eine notwendige Bedingung um das Geheimnis später rekonstruieren zu können. Das Geheimnis ist $k \equiv s (mod\ p_0)$, die einzelnen Shares berechnen sich aus $s_i \equiv s (mod\ p_i)$, für *i=1,...,n*.

Wollen nun *t* Shareholder das Geheimnis wiederherstellen, erhält der Combiner ein System von Kongruenzen:

$$\begin{aligned} s_{i_1} &\equiv s (mod\ p_{i_1}) \\ s_{i_2} &\equiv s (mod\ p_{i_2}) \\ &\vdots \\ &\vdots \\ s_{i_t} &\equiv s (mod\ p_{i_t}) \end{aligned}$$

Mit Hilfe des Chinesischen Restsatzen kann er das System lösen und erhält *s*.

Da laut Voraussetzung $0 < s < \prod_{i=1}^{t} p_i$ gilt, ist die Lösung eindeutig. Mit dem öffentlichen p_0 und dem gewonnenen *s* kann er dann das Geheimnis *k* berechnen.

Ein Beispiel für ein (2,4) Modular-Schema.
Das Geheimnis sei *k=3.* Don wählt $p_0 = 17,\ p_1 = 19,\ p_2 = 23,\ p_3 = 29,\ p_4 = 31$.

$0 < s < \prod_{i=1}^{t} p_i , t = 2$ => $0 < s < Z_{19 \times 23} = Z_{437}$ => ***s=241.***

Es ergeben sich die Shares: $s_1 = 13 \equiv 241 (mod\ 19)$, $s_2 = 11 \equiv 241 (mod\ 23)$,
$s_3 = 9 \equiv 241 (mod\ 29)$, $s_4 = 24 \equiv 241 (mod\ 31)$.

Die Shareholder P_2 und P_4 wollen das Geheimnis rekonstruieren. Clara erhält das Gleichungssystem: $11 \equiv s (mod\ 23)$
$24 \equiv s (mod\ 31)$

Mit dem Chinesischen Restsatz erhalten wir eine Lösung *s=241*.
Zur Berechnung des Geheimnisses $k \equiv 241 (mod\ 17) = 3$ => *k=3*

8 Zusammenfassung

Wir haben eine Reihe von Verfahren kennengelernt, die das von Shamir 1979 aufgeworfene Problem des Secret Sharing lösen können. Die vorgestellten Verfahren bieten die Möglichkeit ein Geheimnis auf mehrere Personen zu verteilen und einem bestimmten Personenkreis die Rekonstruktion zu ermöglichen. Die Schwellwert Schemata eignen sich aber nur bedingt für eine Gewichtung der einzelnen Shareholder. Allgemeinere Zugriffsstrukturen sind mit den vorgestellten Verfahren nicht realisierbar.

Literatur

[1] J. Pieprzyk, T. Hardjono, J. Seberry. *Fundamentals of Computer Security*. Springer, 2003

[2] D. Stinson. *Cryptography: Therory & Practice.* CRC, 2002

[3] A. Shamir. *How to share a secret.* Communications of the ACM, 1979

[4] C. Asmuth, J. Bloom. *A modular approach to key safeguarding.* IEEE Transactions on Information Theory, 1983