Seminar SS 2014

Proseminar Kryptographie

Lehr- und Forschungsgebiet IT-Sicherheit

UMIC Research Centre

Prof. Dr. Ulrike Meyer

Rheinisch-Westfälische Technische Hochschule Aachen

Secret Sharing

Michael Krause (331069)

Aachen, 13.04.2014

Inhaltsverzeichnis

1 Einführung **1**

1.1 Einsatzgebiete 1

1.2 Einfaches Secret Sharing 2

1.3 (n,t)-Schwellenwertschemata 3

2 Shamirs Secret Sharing **4**

2.1 Idee 4

2.2 Verfahren 5

2.3 Sicherheit 7

2.4 Alternatives Verfahren von Blakley 7

2.5 Probleme 8

3 Verifizierbares Secret Sharing **9**

3.1 Idee 9

3.2 Verfahren von Feldmann 9

3.3 Leistungen und Probleme 11

4 Secret Sharing ohne Dealer **11**

4.1 Idee und Verfahren von Ingemarsson und Simmons 11

4.2 Vor- und Nachteile 13

5 Secret Sharing ohne perfekte Sicherheit **13**

5.1 Motivation und Idee 13

5.2 Verfahren von Krawcyk 14

6 Zusammenfassung **14**

Literaturverzeichnis **16**

1 Einführung

Secret Sharing bezeichnet in der Kryptographie das Problem, eine Geheiminformation auf mehrere Geheimnisträger zu verteilen.[4] Es wurde zuerst 1979 in einer Arbeit von George Blakley mit dem Ziel untersucht, eine sichere Methode zum Aufbewahren privater Schlüssel zu finden, welche bei asymmetrischen Verschlüsselungsverfahren wie RSA auftauchen.[3] Blakleys Idee, den privaten Schlüssel an mehrere Hüter zu verteilen, und deren Umsetzung bildet zusammen mit einem weiterem, im selben Jahr durch Adi Shamir veröffentlichtem Verfahren[13], die Grundlage der Forschung im Bereich des Secret Sharing.

In dieser Arbeit werden wir zunächst die Problemstellungen genauer betrachten, die durch Secret Sharing gelöst werden sollen, und dafür eine einfache Lösung vorschlagen. Es wird jedoch deutlich werden, dass in vielen Anwendungsfällen unsere einfache Methode nicht ausreicht und wir somit ein flexibleres Verfahren benötigen. In Folge dessen beschreiben wir Shamirs Secret Sharing und untersuchen dort die Sicherheit, sowie Vorteile und Problempunkte. Schließlich führen wir weitere Verfahren ein, die eben jene Problempunkte behandeln: Zunächst Verifizierbares Secret Sharing, anschließend ein demokratisches und zuletzt ein besonders platzsparendes Verfahren. Wir beschließen die Arbeit mit einem Ausblick auf weitere Forschungen im Bereich des Secret Sharing.

1.1 Einsatzgebiete

Betrachten wir zunächst einige Anwendungen für Secret Sharing.

Eine Dissidentin und eine Journalistin schreiben sich verschlüsselte e-Mails. Da die beiden sensible Informationen austauschen, möchte keine von ihnen die Kommunikation angreifbar machen, indem sie sich ihren privaten Mailschlüssel im Klartext notiert. Allerdings wollen beide die Nachrichten auch dann noch lesen können, wenn sie den Schlüssel vergessen haben. Sie wollen ihre Schlüssel deshalb an verschiedenen Orten aufgeteilt verwahren.

Fünf Biologen haben ein gefährliches Virus entdeckt und einigen sich darauf, die Proben des Virus in einem Tresor aufzubewahren. Keiner der Wissenschaftler soll den Tresor alleine öffnen können, weshalb kein Einzelner das Codewort dazu kennen darf. Stattdessen sollen nur alle fünf gemeinsam in der Lage sein, das Codewort zu bestimmen, mit dem die Tür sich öffnet.

Bei beiden Beispielen handelt es sich um typische Anwendungsfälle für Secret Sharing. Im ersten Fall muss eine wichtige Information (der private Schlüssel) gespeichert werden. In zweitem Fall wird eine Zugangskontrolle benötigt, die auf eine Gruppe von Personen reagiert. Auch hier gibt es eine Geheiminformation: das Codewort zum Öffnen des Schlosses. In beiden Fällen darf das Geheimnis nicht verloren gehen. Gleichzeitig ist es nicht praktikabel, das Geheimnis an mehreren Stellen aufzubewahren: dies bietet einem potentiellen Angreifer mehr Einfallstore.[13]

Allgemein ist Secret Sharing bei allen Situationen hilfreich, in denen besonders wichtige Informationen gesichert werden müssen - Geheimrezepte, Zugangscodes, Dokumente. Zur Offenlegung der Information sind dabei immer mehrere Geheimnisteile nötig. Diese können an verschiedenen Orten vorliegen, insbesondere also an verschiedene Personen weitergegeben werden. Dass die Information erst aus mehreren Quellen zusammengesetzt werden muss, macht es unwahrscheinlicher, dass sie in falsche Hände gelangt.[4]

Es gibt jedoch auch Situationen, in denen Secret Sharing nicht hilfreich ist. Dies ist etwa der Fall, wenn nicht genug sichere Verwahrungsorte bzw. vertrauenswürdige Personen zur Verfügung stehen. Ebenso schlägt das Konzept fehl, wenn es keine Möglichkeit gibt, die Geheimnisteile an ihren Verwahrungsort zu bringen. Dies geschieht insbesondere in einer überwachten Umgebung, in der überhaupt keine sichere Kommunikation zu anderen Personen möglich ist.[6]

1.2 Einfaches Secret Sharing

Alice möchte ein Geheimnis S an t Freunde verteilen. Jedes Teilgeheimnis an sich soll ohne Wert sein, nur mit allen t Teilen soll Alices Geheimnis aufgedeckt werden können. Wir nennen Alice *Dealer* und ihre Freunde *Insider*.[4]

Nun gehen wir davon aus, dass Alice S als Binärzahl vorliegen hat oder es als solche kodieren kann. Ein Beispiel wäre etwa der Zugangscode für Alices Haustür. Sollte sie den Code vergessen, könnten ihre Freunde ihr aushelfen.

Um S zu verteilen, erzeugt Alice $t-1$ zufällige Binärzahlen der selben Länge wie S. Diese Zufallszahlen $(S_1 \dots S_{t-1})$ stellen die Geheimnisteile dar, wobei sich der letzte Geheimnisteil als XOR-Verknüpfung der anderen Teile zusammen mit S ergibt $(S_t = S \oplus S_1 \oplus S_2 \oplus \cdots \oplus S_{t-1})$. Alices Freunde erhalten jeweils einen Geheimnisteil und können S durch eine XOR-Verknüpfung all ihrer Geheimnisteile bestimmen $(S = S_1 \oplus S_2 \oplus \cdots \oplus S_t)$.[12][7]

Beispiel 1.1. Für drei Geheimnisträger:

$$\begin{aligned} S &= 0110110001011000 \\ S_1 &= 1100101111011100 \\ S_2 &= 1000110011101111 \\ S_3 = S \oplus S_1 \oplus S_2 &= 0010101101101011 \end{aligned}$$

Bei diesem Verfahren reichen weniger als t Geheimnisteile nicht aus, um S herauszufinden. Tatsächlich liefern sie keine Information über die Beschaffenheit von S, außer dessen Länge.[12]

Dazu folgende Überlegung: Wir müssen nur den Fall untersuchen, in dem $t-1$ Geheimnisteile vorliegen, da dies offensichtlich das Maximum an Information darstellt, ohne dass t Teile bekannt sind. Da allerdings bei $t-1$ vorhandenen Teilen der letzte erforderliche Geheimnisteil potentiell jede zu S gleichlange Binärzahl sein könnte, kann auch durch XOR-Verknüpfung jede Binärzahl als Geheimnis S entstehen. $t-1$ Geheimnisteile ermöglichen also keinen Rückschluss auf das Geheimnis. Diese Eigenschaft eines Secret Sharing Verfahrens nennen wir *perfekte Sicherheit.*[12]

Natürlich ergibt sich aus der perfekten Sicherheit unmittelbar der Nachteil, dass kein Geheimnisteil verloren gehen darf - sonst kann das Geheimnis nicht rekonstruiert werden. Diesen Nachteil wollen wir im Folgenden durch ein ausgefeilteres Verfahren beheben.

1.3 (n,t)-Schwellenwertschemata

Als *(n,t)-Schwellenwertschema* bezeichnen wir Secret Sharing, bei dem ein Geheimnis S in n Teile geteilt wird, von denen mindestens t erforderlich sind, um S zu rekonstruieren.[4] t ist hier also ein „Schwellenwert“, ab welchem S bekannt ist.[2][1] Das zuvor besprochene Verfahren könnten wir als (n, n)-Schema beschreiben.

In einem (n, t)-Schema können bis zu $n - t$ Geheimnisteile verloren gehen oder höchstens $t - 1$ Geheimnisteile von einem Angreifer abgefangen werden, ohne dass das Geheimnis in Gefahr gerät.[13] In einem Schwellenwertschema können außerdem einige Geheimnisträger gegenüber anderen bevorzugt werden, indem sie mehrere Geheimnisteile zugewiesen bekommen.[12][13] Damit sind die (n, t)-Schemata deutlich flexibler als das zuletzt vorgestellt Verfahren.

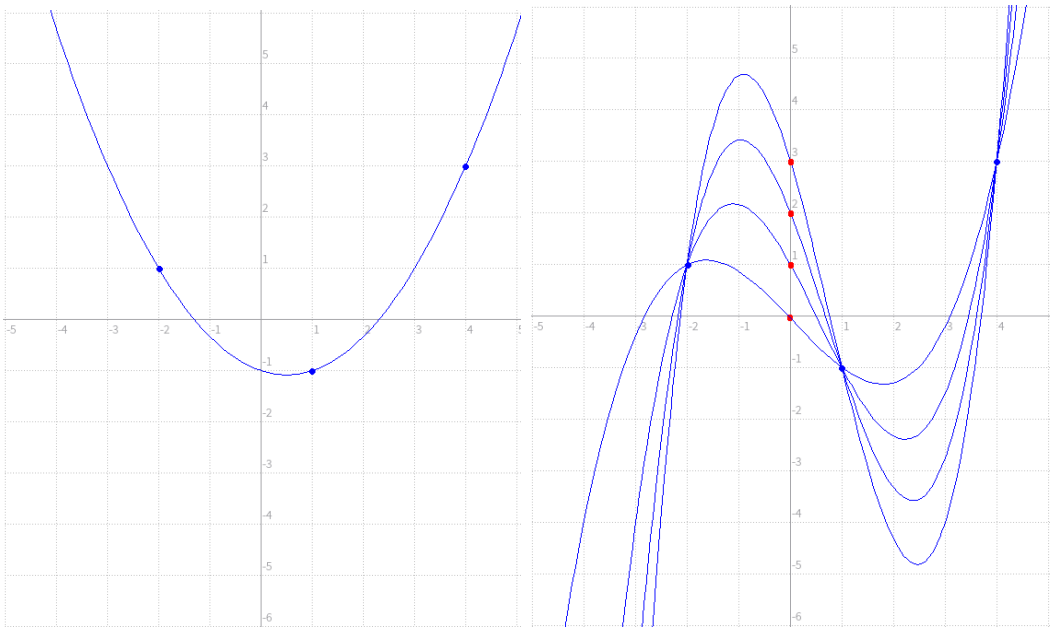
Wir wollen nun anhand eines von Shamir entwickelten Verfahrens die Implementierung eines Schwellenwertschemas genauer betrachten. Zudem beschreiben wir kurz ein alternatives Verfahren nach Blakley.

2 Shamirs Secret Sharing

2.1 Idee

Die zentrale Idee von Shamirs Secret Sharing basiert auf folgendem Satz:

Satz 2.1. Durch t Punkte in der zweidimensionalen Ebene wird ein Polynom vom Grad höchstens $t-1$ eindeutig bestimmt. (vgl. [4], leicht verändert)



(a) Hier wird eine Parabel durch drei Punkte eindeutig bestimmt

(b) Erst durch einen weiteren Punkt wird ein Polynom vom Grad drei eindeutig festgelegt

Abbildung 1: Anschauliche Darstellung von Satz 2.1

Beweis. (vgl. [4], leicht verändert) Wir betrachten das Polynom $P(x) = \sum_{k=0}^{t-1} a_k x^k$ und außerdem paarweise verschiedene $x_i, \forall 1 \leq i \leq t$, sowie $y_i = P(x_i)$.

Durch Einsetzen der x_i, y_i in die Polynomgleichung ergibt sich das Gleichungssystem:

$$\begin{aligned} a_0 + x_1 a_1 + {x_1}^2 a_2 + \cdots + {x_1}^{t-1} a_{t-1} &= y_1 \\ a_0 + x_2 a_1 + {x_2}^2 a_2 + \cdots + {x_2}^{t-1} a_{t-1} &= y_2 \\ &\cdots \\ a_0 + x_t a_1 + {x_t}^2 a_2 + \cdots + {x_t}^{t-1} a_{t-1} &= y_t \end{aligned}$$

Dieses Gleichungssystem lässt sich schreiben als:

$$\begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{t-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{t-1} \\ \vdots & & \ddots & & \vdots \\ 1 & x_t & x_t^2 & \cdots & x_t^{t-1} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{t-1} \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_t \end{pmatrix}$$

Hierbei ist der erste Faktor eine Vandermonde-Matrix. Für diese kennen wir die Determinante: $det = \prod_{1 \le i < j \le t} (x_j - x_i)$

Da x_j und x_i paarweise verschieden nach Voraussetzung, ist $det \neq 0$. Also ist die Matrix regulär und damit das Gleichungssystem eindeutig lösbar. □

Shamir weißt ausdrücklich darauf hin, dass anstatt Polynomen auch beliebige andere Funktionen verwendet werden können, die die Eigenschaft des Satzes 2.1 aufweisen und schnell auszuwerten sind.[13]

Anschaulich gesprochen funktioniert Shamirs Secret Sharing so: n Insider erhalten durch den Dealer paarweise verschiedene Punkte auf einem Polynom vom Grad $t-1$, dessen konstanter Term das Geheimnis S ist. Dann können t Insider das Polynom (und damit auch S) rekonstruieren, womit ein (n, t)-Schwellenwertschema umgesetzt ist.

2.2 Verfahren

Alice möchte ihr Geheimnis S durch ein (n, t)-Schwellenwertschema nach Shamir verteilen. Sie wählt dazu eine Primzahl p, sodass $S \in \mathbb{Z}_p$ darstellbar ist und $n < p$. Außerdem bestimmt sie ein Polynom $P(x) = S + \sum_{j=1}^{t-1} a_j x^j, a_j \in \mathbb{Z}_p$ mit beliebigen Koeffizienten a_j sowie paarweise und von 0 verschiedene $x_i \in \mathbb{Z}_p, 1 \le i \le n$ (wegen $n < p$ gibt es entsprechend viele x_i). Zuletzt berechnet sie zu jedem x_i ein y_i, sodass $y_i = P(x_i)$. Die Paare (x_i, y_i) bezeichnen also Punkte auf $P(x)$.[4][13][12]

Die y_i sind die Geheimnisteile. Jeder Insider muss durch Alice eines dieser Teilgeheimnisse sicher übermittelt erhalten. Die x_i veröffentlicht Alice, da sie keine sensiblen Informationen tragen. Jedem Insider muss jedoch die Zuordnung zwischen seinem Geheimnisteil und dem entsprechenden x_i bekannt sein. Außerdem veröffentlicht Alice p, damit die Insider in $\mathbb{Z}_p$ rechnen können.[12] Damit ist Alice fertig.

Zur Rekonstruktion von S finden sich nun t Geheimnisträger zusammen. Nach Satz 2.1 haben sie genug Informationen, um Alices Polynom zu bestimmen. Sie können dazu das vorgestellte Gleichungssystem lösen, was allerdings rechnerisch sehr aufwendig sein kann.[7] Alternativ benutzen sie die Langrangsche Interpolationsformel:[4]

$$P(x) = \sum_{i=1}^{t} y_i \prod_{j=1, j\neq i}^{t} \frac{x_j - x}{x_j - x_i} \tag{1}$$

Beziehungsweise, da nur der konstante Term gesucht ist:[4]

$$S = \sum_{i=1}^{t} y_i \prod_{j=1, j\neq i}^{t} \frac{x_j}{x_j - x_i} \tag{2}$$

Beispiel 2.1. Alice möchte ein (5,3)-Schema aufsetzen. Ihr Geheimnis ist $S = 20$. Sie wählt $p = 23$ und als Polynom $P(x) = 20 + 12x + 6x^2$.

Nun nimmt Alice fünf Stellen auf dem Polynom: $x_1 = 1, x_2 = 2, x_3 = 3, x_4 = 4, x_5 = 5$. Daraus berechnet sie die Geheimnisteile:

$$y_1 = P(x_1) = P(1) = 20 + 12 * 1 + 6 * 1^2 \bmod 23 = 15$$

Und analog: $y_2 = 22, y_3 = 18, y_4 = 3, y_5 = 0$ Die y_i werden als Teilgeheimnisse an die Insider übertragen.

Nun finden sich die Insider mit den Geheimnisteilen y_1, y_2 und y_3 zusammen, um S zu rekonstruieren. Dazu verwenden sie Gleichung 2:

$$S = \sum_{i=1}^{3} y_i \prod_{j=1, j\neq i}^{3} \frac{x_j}{x_j - x_i} =$$
$$15 * \frac{2}{2-1} * \frac{3}{3-1} + 22 * \frac{1}{1-2} * \frac{3}{3-2} + 18 * \frac{1}{1-3} * \frac{2}{2-3} \bmod 23 = 20$$

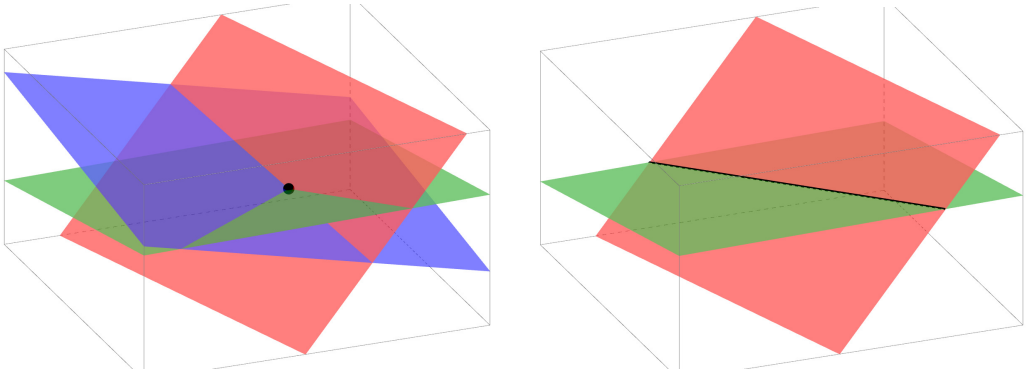
2.3 Sicherheit

Im Abschnitt 1.2 konnten wir einfach argumentieren, dass das Secret Sharing mittels XOR-Verknüpfung perfekt sicher sei. Etwas ähnliches ist auch bei Shamirs Secret Sharing möglich: Angenommen, ein Angreifer kennt $t-1$ Geheimnisteile und noch ein Teil ist nötig, um das Polynom zu konstruieren. Für jedes mögliche Geheimnis (also jedes Element von $\mathbb{Z}_p$) ergibt sich zusammen mit den $t-1$ vorliegenden Teilen *genau ein* Polynom vom Grad t. Also sind auch alle Geheimnisse gleich wahrscheinlich.[4][13]

Anschaulich lässt sich das anhand einer Grafik begreifen: Liegen $t-1$ Punkte vor, lässt sich ein beliebiger Punkt mit $x=0$ hinzunehmen, um ein Polynom vom Grad $t-1$ aufzustellen - und jeder dieser Punkte ist als Geheimnis gleich wahrscheinlich (vgl. auch Abbildung 1). Bei dieser Analogie ist allerdings nicht zu vergessen, dass bei Shamir mit diskreten Werten gerechnet wird, die Darstellung aber im reellen Zahlenraum ist.

Für einen Angreifer, der überhaupt keine Geheimnisteile besitzt, sind ebenfalls alle Geheimnisse gleich wahrscheinlich. Shamirs Secret Sharing ist deshalb perfekt sicher.[12] Allerdings sind natürlich große p notwendig, um die Gefahr zu verringern, dass S erraten werden kann.[2]

2.4 Alternatives Verfahren von Blakley



(a) (b)

Abbildung 2: Secret Sharing nach Blakley

Im gleichen Jahr wie Shamir hat George Blakley sein Verfahren zur Umsetzung eines Schwellenwertschemas veröffentlicht.[3] Hier wird das Geheimnis nicht als Glied eines Polynoms dargestellt, sondern als Punkt im t-Dimensionalen Raum.[12] Das Verfahren basiert also auf geometrischen Überlegungen.

Jeder der n Insider erhält als Geheimnisteil eine (Hyper-)Ebene in diesem Raum zugewiesen, die den geheimen Punkt enthält. Blakley argumentiert nun, dass sich t dieser Ebenen mit hoher Wahrscheinlichkeit in genau diesem einen Punkt im Raum schneiden.[3] Indem also die t Insider den Schnittpunkt ihrer Ebenen bestimmen, rekonstruieren sie das Geheimnis (siehe auch Abbildung 2(a)).[12]

Blakleys Secret Sharing kann analog zu Shamirs Schema eingesetzt werden. Es gibt jedoch im Wesentlichen zwei Unterschiede: Zunächst ist Blakleys Verfahren nicht ganz so effizient[13], d.h: die Größe eines Geheimnisteils ist grundsätzlich größer, als die des Geheimnisses. Um einen Geheimnisteil - eine Hyperebene - zu bestimmen, sind mehr Informationen nötig, als um das Geheimnis - einen Punkt - festzulegen.[8] Im Gegensatz dazu, sind bei Shamir die Geheimnisteile und das Geheimnis selbst Elemente des selben endlichen Körpers, d.h: ihre Darstellung verbraucht gleich viel Platz.[13]

Des Weiteren ist Blakleys Schema nicht perfekt sicher. Ein Außenstehender weiß nur, dass sich der geheime Punkt irgendwo im Raum befinden kann. Ein Insider kann dies eingrenzen, denn er weiß, dass der Punkt in seiner Ebene liegt. Mehrere Insider zusammen können durch die Schnitte ihrer Ebenen die möglichen Punkte weiter eingrenzen (siehe auch Abbildung 2(b)).[8]

Blakleys Überlegungen zum geometrischen Secret Sharing spielen eine wichtige Rolle bei der Umsetzung komplexer Zugriffsstrukturen, die wir im Schlussteil kurz betrachten werden.

2.5 Probleme

Obwohl Shamirs Secret Sharing perfekt sicher ist, treten in der Praxis Probleme auf. Verwendet der Dealer etwa einen unsicheren Zufallszahlengenerator zum Erzeugen der Koeffizienten des geheimen Polynoms, könnte ein Angreifer unter Umständen das Polynom erraten. Außerdem ist der Dealer zum Übermitteln der Teilgeheimnisse an die Insider auf einen sicheren Kommunikationskanal angewiesen. Die Sicherheit dieses Kanals beschränkt also auch die Sicherheit des gesamten Verfahrens.

Weitere Probleme entstehen durch regelwidriges Verhalten der Beteiligten. So könnte der Dealer etwa falsche Geheimnisteile an einige Insider verschicken, um einige Insider gegenüber anderen zu privilegieren.[1] Die Insider könnten ihre Teilgeheimnisse zurückhalten oder falsche Werte in die Rekonstruktion einbringen - ohne, dass dies bemerkt wird.[1][12] Da bei der Rekonstruktion jeder sein Teilgeheimnis öffentlich

macht, kann ein Lügner unter den Insidern die Teile der anderen Abgreifen und das Geheimnis für sich selbst berechnen.[12]

Wir wollen einige dieser Schwierigkeiten durch sogenanntes Verifizierbares Secret Sharing beheben.

3 Verifizierbares Secret Sharing

3.1 Idee

Betrug beim Secret Sharing wird erschwert, wenn die Insider eine Möglichkeit haben, die Korrektheit ihres Teilgeheimnisses und der behaupteten Geheimnisse eines Anderen zu kontrollieren.[1] Wir wollen das Verfahren für verifizierbares Secret Sharing nach Paul Feldmann betrachten.[5] Dabei werden durch den Dealer Prüfwerte berechnet, die von den Insidern zum Vergleich ihrer Teilgeheimnisse herangezogen werden können.

Die Funktion, mittels der diese Prüfwerte berechnet werden, muss eine homomorphe Einwegfunktion sein[1][5]. Für solche Funktionen lässt sich die Umkehrabbildung nur schwer finden, außerdem lässt sich auf den Bildern der Funktion rechnen, sodass Beziehungen zwischen den entsprechenden Urbildern erhalten bleiben. Beide Eigenschaften werden wir ausnutzen.

Eine in der Kryptographie häufig verwendete homomorphe Einwegfunktion ist die diskrete Exponentialfunktion, die auch wir verwenden werden. Ihre Umkehrfunktion - der diskrete Logarithmus - ist schwer zu berechnen.[4] Außerdem gilt:[5]

$$exp(x + y) = exp(x) * exp(y) \tag{3}$$

3.2 Verfahren von Feldmann

Beim verifizierbaren Secret Sharing nach Feldmann bleiben die Berechnungen für Dealer und Insider entsprechend Shamirs Verfahren gleich. Zusätzlich stellt allerdings der Dealer nach dem Austeilen der Geheimnisteile noch deren Prüfwerte und die Prüfwerte der Koeffizienten des Polynoms (insbesondere also auch von S) öffentlich bereit. Zuletzt verbreitet der Dealer die Basis b und die Primzahl q, die er für die Berechnungen mit der diskreten Exponentialfunktion gewählt hat, damit die Insider die Berechnungen nachvollziehen können.[1][5]

Sobald nun die Insider ihre Geheimnisse erhalten, können sie deren Prüfwerte berechnen und mit den veröffentlichten Werten des Dealers vergleichen. Dasselbe können sie analog bei der Rekonstruktion des Geheimnisses tun, um zu prüfen, ob alle beigesteuerten Werte korrekt sind.[1][5]

Die Teilnehmer sollten allerdings auch die Korrektheit der vom Dealer veröffentlichten Prüfwerte der Teilgeheimnisse prüfen. Dazu vergleichen sie folgende Kongruenz:[1][5]

$$exp(y_i) \equiv_q exp(P(x_i)) \equiv_q exp(\sum_{k=0}^{t-1} a_k x_i^k) \overset{3}{\equiv}_q \prod_{k=0}^{t-1} exp(a_k x_i^k) \equiv_q \prod_{k=0}^{t-1} exp(a_k)^{x_i^k} \quad (4)$$

Beispiel 3.1. Alice möchte ihr (5,3)-Schema aus Beispiel 2.1 erweitern. Zur Erinnerung:

$$p = 23, S = 20, a_1 = 12, a_2 = 6, P(x) = 20 + 12x + 6x^2$$
$$x_1 = 1, x_2 = 2, x_3 = 3, x_4 = 4, x_5 = 5$$
$$y_1 = 15, y_2 = 22, y_3 = 18, y_4 = 3, y_5 = 0$$

Alice wählt eine Primzahl q, sodass p ein Element der Primfaktorzerlegung von $q-1$ ist[5], zum Beispiel $q = 47$. Sie berechnet die Prüfwerte mit Hilfe der diskreten Exponentialfunktion zur Basis $b = 7$ in $\mathbb{Z}_q$:

$$exp(a_1) = b^{a_1} \bmod q = 7^{12} \bmod 47 = 17$$
$$\text{und analog: } exp(a_2) = 8, exp(S) = 37,$$
$$exp(y_1) = 3, exp(y_2) = 27, exp(y_3) = 42, exp(y_4) = 14, exp(y_5) = 1$$

Die Insider sollten die Kongruenz 4 prüfen:

$$exp(y_1) \equiv_q \prod_{k=0}^{t-1} exp(a_k)^{x_1^k} \equiv_q exp(S) * exp(a_1)^{x_1} * exp(a_2)^{x_1^2} \equiv_q 37 * 17^1 * 8^{1^2} \equiv_q 3$$
$$exp(y_2) \equiv_q \prod_{k=0}^{t-1} exp(a_k)^{x_2^k} \equiv_q exp(S) * exp(a_1)^{x_2} * exp(a_2)^{x_2^2} \equiv_q 37 * 17^2 * 8^{2^2} \equiv_q 27$$

(und analog für $exp(y_3) \dots exp(y_5)$)

Die Schwindlerin Mallory behauptet, sie sei die dritte Teilnehmerin und ihr Geheimnis laute $y_3' = 10$. Die anderen können jedoch feststellen, dass dies nicht stimmen kann, denn es ist:

$$exp(y_3) \equiv_q 42 \not\equiv_q 32 \equiv_q 7^{10} \bmod 47 \equiv_q exp(y_3')$$

3.3 Leistungen und Probleme

Feldmanns Verfahren bietet für die Insider eine gute Möglichkeit, die Korrektheit von Teilgeheimnissen zu prüfen. Da der Dealer nur einige zusätzliche Informationen veröffentlichen muss, lässt es sich sehr leicht auf ein bestehendes Secret Sharing Schema aufsetzen und ist einfach zu implementieren. Fraglich ist bei der Implementierung allerdings, wie die Teilnehmer auf einen lügnerischen Dealer oder Insider reagieren sollen. Feldmann behandelt diese Frage nicht.[5]

Die Sicherheit des Verfahrens hängt ganz entscheidend von der verwendeten Einwegfunktion ab. Es sollte nicht möglich sein, aus dem veröffentlichten Prüfwert von S das eigentliche Geheimnis zu berechnen.

In unserem Beispiel basiert die Sicherheit also auf dem Problem, den diskreten Logarithmus in endlichen Körpern zu berechnen. Feldmann empfiehlt zur Verbesserung der Sicherheitseigenschaften etwa den Einsatz von elliptischen Kurven oder von Verkettungen mehrerer Einwegfunktionen.[5]

Einige der in Abschnitt 2.5 beschriebenen Probleme bleiben bestehen. Schlechte Zufallszahlen und unsichere Kommunikationswege werden durch Verifizierbares Secret Sharing nicht abgedeckt, auch können die Insider ihre Teilgeheimnisse weiterhin für sich behalten. Und auch wenn die Insider nun bei dem Versuch, falsche Werte zur Rekonstruktion von S beizusteuern, erwischt werden können, könnten sie vorher dennoch die Geheimnisse anderer Insider erfahren haben.

4 Secret Sharing ohne Dealer

4.1 Idee und Verfahren von Ingemarsson und Simmons

Wir sind bisher von dem Fall ausgegangen, in dem ein Dealer ein Geheimnis per Secret Sharing verteilen möchte. Es gibt aber Situationen, in denen eine Geheiminformation überhaupt keiner Person bekannt sein soll. Sinnvollerweise ist dies keine Information, die einen Wert *an sich* hat, sondern die etwas auslöst - beispielsweise ein Code, der einen Safe öffnet.

Ingemar Ingemarsson und Gustavus Simmons haben ein Verfahren zum Secret Sharing ohne Dealer entwickelt, das sie auch als *demokratisches* Secret Sharing bezeichnen (im Gegensatz zum *autokratischem* Geheimnis teilen durch einen Dealer). Hierbei bekommt jeder Insider gleichen Einfluss auf die Bestimmung des Geheimnisses, kann seinen Einfluss aber - freiwillig - an andere Insider abgeben.[8]

Zunächst wählt jeder Insider ein eigenes, zufälliges Geheimnis. Die persönlichen Geheimnisse übermittelt dann jeder Insider an einen Mechanismus, der aus den Eingaben eine Summe bildet. Sind die Geheimnisse Binärzahlen, bietet sich also eine XOR-Verknüpfung an, ähnlich unserem Beispiel aus Abschnitt 1.2. Der Mechanismus soll anschließend genau dann reagieren, wenn sich durch erneute Eingaben wieder die vorherige Summe bildet. Auf die genaue Ausgestaltung des Mechanismus gehen Ingemarsson und Simmons nicht ein.[8]

Mit Hilfe des Mechanismus haben die Insider ein demokratisches (n, n)-Schema umgesetzt. Dieses können sie nun zu beliebigen (n, t)-Schemata ausgestalten, indem jeder von ihnen sein persönliches Geheimnis durch klassisches Secret Sharing an die anderen Insider verteilt. Dementsprechend kann jeder entscheiden, wem er einen Teil seines persönlichen Geheimnisses anvertraut, und wem nicht.[8]

Beispiel 4.1. Die Biologen Bob, Carol, Dora, Emil und Fred haben eine neurotoxische Pflanze entdeckt und sichern sie hinter einer Stahltür. Keiner von ihnen soll die Tür alleine öffnen können, außerdem traut nicht jeder Biologe jedem. Insbesondere traut Bob niemand anderem: Er will auf jeden Fall dabei sein, wenn die Tür geöffnet wird.

Die Fünf setzen zuerst ein (n, n)-Schema auf, indem jeder sein persönliches Geheimnis an dem Codeschloss der Stahltür verdeckt eingibt. Das Codeschloss speichert dann die Verknüpfung der Eingaben. Anschließend verteilen sie ihre Teilgeheimnisse entsprechend folgender Abbildung:

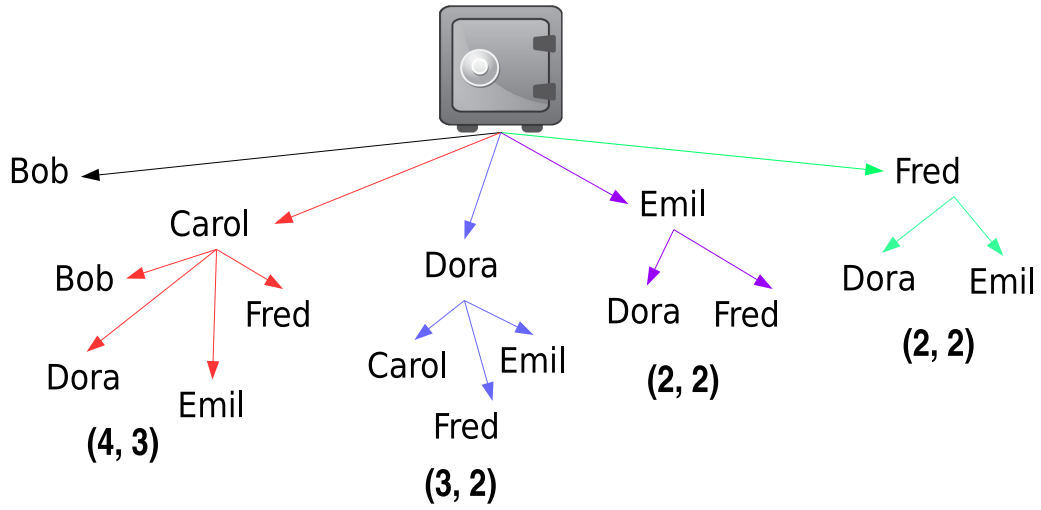


Abbildung 3: Vertraunsnetz bei demokratischem Secret Sharing

Demnach vertraut Carol den anderen Wissenschaftlern und verteilt ihr Teilgeheimnis durch ein (4,3)-Schema. Emil und Fred trauen nur dem jeweils anderen, sowie Dora

und setzen entsprechend (2,2)-Schemata auf. Bob verteilt sein Teilgeheimnis nicht, weshalb die anderen die Tür nie ohne ihn öffnen können.

4.2 Vor- und Nachteile

Demokratisches Secret Sharing kann das klassische Verfahren nach Shamir bei Kontrollmechanismen wie Tür- oder Safeschlössern ersetzen. Je nach den Anforderungen der Teilnehmer sind beliebig komplexe Vertrauensnetze möglich. Dabei muss niemand eine Kontrollgruppe erlauben, die er selbst für zu schwach hält.[8]

Andererseits sind nicht unbedingt alle Beteiligten mit den sich ergebenden Kontrollkonstellationen zufrieden. Im Beispiel 4.1 würden es vielleicht die Meisten bevorzugen, wenn auch Bob sein Teilgeheimnis weitergäbe.

Eine Schwachstelle des Verfahrens ist der Mechanismus, der die Summe der Teilgeheimnisse speichert. Im Gegensatz zum Dealer in klassischem Secret Sharing funktioniert dieser Mechanismus zwar ohne Zufallszahlen und sichere Kommunikationswege (wenn z.B. die Codes direkt und verdeckt am Türschloss eingegeben werden), jedoch muss sichergestellt werden, dass ein Angreifer den Mechanismus nicht manipulieren oder umgehen kann.

5 Secret Sharing ohne perfekte Sicherheit

5.1 Motivation und Idee

Wir haben mit Shamirs Secret Sharing ein sicheres Verfahren zum Teilen von Geheimnissen kennengelernt. Dabei haben wir aber ein praktisches Problem noch nicht betrachtet: Verteilt ein Dealer ein besonders großes Geheimnis, sammeln sich auch bei den Insidern sehr große Datenmengen an. Da das Geheimnis und dessen Teile als Elemente des selben endlichen Körpers dargestellt werden, haben ihre Darstellungen den selben Speicherplatzverbrauch. [9]

Angenommen, das Geheimnis ist 100 MB groß. Wenn 10 Personen einen Teil erhalten sollen, bedeutet das einen Speicherplatzverbrauch von insgesamt 1 GB über alle Teilnehmer gerechnet. Dies stellt vor allem bei der Übertragung der Teilgeheimnisse zu den Insidern ein Problem dar. Weiterhin müssen die an der Rekonstruktion eines Geheimnisses teilhabenden Insider all ihre Teile zusammentragen - je nach dem zu Grunde liegenden Kommunikationsnetz kann dies sehr schwierig und langsam sein.

Hugo Krawcyk schlägt in seiner Arbeit vor, die bei Shamir gegebene perfekte Sicherheit zu Gunsten deutlich kleinerer Geheimnisteile aufzugeben.[9] Dieser Schritt liegt nahe, da eine vollständige perfekte Sicherheit in der Praxis durch schwache Zufallszahlengeneratoren und unsichere Kommunikationswege im Allgemeinen nicht gegeben ist.

5.2 Verfahren von Krawcyk

Krawcyks Vorschlag ist einfach: Statt das Geheimnis S zu verteilen, wird S verschlüsselt und nur der dazu verwendete Schlüssel k durch Secret Sharing aufgeteilt. Nun muss allerdings noch der Chiffriertext C, der aus S entsteht, sinnvoll verteilt werden. Krawcyk wendet dazu Reed Solomon Fehlerkorrekturcodes an. Dies können wir leicht nachvollziehen, da diese Codes auf dem selben Satz 2.1 wie bereits Shamirs Verfahren basieren.[9]

Der Chiffriertext C soll in n Teile gespalten werden, sodass er mit t von n Teilen wiederhergestellt werden kann. Sicherheit spielt dabei keine Rolle, denn wenn ein Angreifer von C erfährt, bräuchte er immer noch den Schlüssel k, um C zu entschlüsseln. Dementsprechend können wir wieder Shamirs Verfahren anwenden (d.h: ein Polynom konstruieren), mit dem Unterschied, dass diesmal nicht ganz C als konstanter Term des Polynoms gewählt wird. Stattdessen wird C in t gleich große Teile geteilt und jeder dieser Teile als ein Koeffizient des Polynoms verwendet. Im Ergebnis speichern wir t-mal mehr Information in einem Polynom als bei Shamir. Somit hat jeder Teil von C die Größe $\frac{|C|}{t}$.[9]

Der Dealer gibt jedem Insider einen Teil von k und einen Teil von C, wobei nur der Schlüsselteil gesichert übertragen und aufbewahrt werden muss. Allerdings erfährt ein Angreifer das Geheimnis S, wenn er C zusammensetzen und entschlüsseln kann. Die Sicherheit hängt demnach von der Verschlüsselung ab, die für C gewählt wurde.[9]

Der Speicherplatzverbrauch beträgt bei jedem Insider $\frac{|C|}{t}+|k|$ statt S bei klassischem Secret Sharing und über alle Insider verteilt $\frac{n}{t} * |C| + n * |k|$ statt $n * |S|$.[9]

6 Zusammenfassung

Wir haben in dieser Arbeit die Idee vom Secret Sharing - dem Teilen von Geheimnissen - sowie mögliche Anwendungen kennengelernt. Neben einem einfachen Secret Sharing Schema haben wir Adi Shamirs Schwellenwertverfahren betrachtet und darauf aufbauend Verifizierbares Secret Sharing nach Paul Feldmann, Demokratisches

Secret Sharing nach Ingemarsson und Simmons sowie das verkürzende Verfahren von Hugo Krawcyk.

Mit diesen Betrachtungen ist allerdings das Forschungsfeld Secret Sharing noch nicht erschöpft. Zu den meisten vorgestellten Verfahren sind Alternativen vorgeschlagen worden, beispielsweise hat Pedersen die Idee von Feldmann verfeinert und - zumindest auf Seiten der Insider - perfekt sicher gemacht.[11]

Zum Schluss wollen wir noch drei Forschungsfelder anschneiden, die bisher überhaupt nicht erwähnt wurden.

Mit komplexeren Zugriffsstrukturen, also Secret Sharing Schemata, die genauere Kontrolle über S erlauben, als dies bei (n,t)-Schemata möglich ist, beschäftigt sich unter anderem Simmons.[14] Seine Secret Sharing Modelle sind geometrisch und orientieren sich damit etwas an dem Verfahren von Blakley. Mit ihnen ist es etwa möglich, ein Unternehmensgeheimnis für eine Gruppe von Mitarbeitern zugänglich zu machen, die jeweils ein Mitglied jeder Abteilung des Unternehmens beinhaltet, aber niemals für eine beliebige Anzahl von Mitarbeitern der selben Abteilung allein.[12][2][1]

Ein weiteres Gebiet sind sogenannte Threshold-Signaturen. Wir nehmen an, dass ein Schlüssel per Secret Sharing verteilt werden soll, mit dem es möglich ist, Nachrichten zu signieren. Verwenden wir dabei die uns bekannten Verfahren, ist nach der einmaligen Rekonstruktion des Geheimnisses der Schlüssel allen beteiligten Insidern bekannt und jeder von ihnen kann Nachrichten signieren. Bei Threshold-Signaturen wird stattdessen eine Nachricht nacheinander von mehreren Insidern unterschrieben und gilt erst ab einem bestimmten Schwellwert als signiert. Dabei muss kein Insider den gesamten Schlüssel erfahren.[1][12]

Bei sogenanntem visuellem Secret Sharing sind sowohl das Geheimnis als auch die Geheimnisteile Bilder. Im einfachsten Fall erhält jeder Insider eine Folie, auf der nur Rauschen (d.h: scheinbar zufällige Bildpunkte) zu sehen ist. Legen die Insider ihre Folien allerdings übereinander, ergibt sich aus den Punkten ein Bild - das Geheimnis. Zum Zusammensetzen ist hier also keine Rechnung erforderlich.[10]

Natürlich stellen diese drei Beispiele nur eine Auswahl dar. Secret Sharing ist ein vielfach untersuchtes Themengebiet und es ist auch in Zukunft spannende, neue Forschung zu erwarten.

Literatur

[1] Beutelspacher, Albrecht ; Neumann, Heike B. ; Schwarzpaul, Thomas: *Kryptografie in Theorie und Praxis - Mathematische Grundlagen für Internetsicherheit, Mobilfunk und elektronisches Geld.* 2. Vieweg + Teubner, 2010. – 252–259 S. – ISBN 978–3–8348–0977–3

[2] Beutelspacher, Albrecht ; Schwenk, Jörg ; Wolfenstetter, Klaus-Dieter: *Moderne Verfahren der Kryptographie - von RSA zu Zero-Knowledge.* 7. Vieweg + Teubner, 2010. – 70–73 S. – ISBN 978–3–8348–1228–5

[3] Blakley, G.R.: Safeguarding cryptographic keys. In: *Proceedings of the 1979 AFIPS National Computer Conference*, AFIPS Press, 1979, S. 313–317

[4] Buchmann, Johannes: *Einführung in die Kryptographie.* 5. Springer, 2010. – 247–250 S. – ISBN 978–3–642–11185–3

[5] Feldman, Paul: A Practical Scheme for Non-interactive Verifiable Secret Sharing. In: *Proceedings of the 28th Annual Symposium on Foundations of Computer Science*, IEEE Computer Society, 1987 (SFCS '87). – ISBN 0–8186–0807–2, S. 427–438

[6] Ferguson, Niels ; Schneier, Bruce ; Kohno, Tadayoshi: *Cryptography Engineering - Design Principles and Practical Applications.* Wiley, 2010. – 310–311 S. – ISBN 978–0–470–47424–2

[7] Freiermuth, Karin ; Hromkovič, Juraj ; Keller, Lucia ; Steffen, Björn: *Einführung in die Kryptologie - Lehrbuch für Unterricht und Selbststudium.* 1. Vieweg + Teubner, 2010. – 358–363 S. – ISBN 978–3–8348–1005–2

[8] Ingemarsson, Ingemar ; Simmons, Gustavus J.: A Protocol to Set Up Shared Secret Schemes Without the Assistance of Mutually Trusted Party. In: *Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques on Advances in Cryptology*, Springer-Verlag New York, Inc., 1991 (EUROCRYPT '90). – ISBN 0–387–53587–X, S. 266–282

[9] Krawczyk, Hugo: Secret Sharing Made Short. In: *Proceedings of the 13th Annual International Cryptology Conference on Advances in Cryptology*, 1993 (CRYPTO '93), S. 136–146

[10] Naor, Moni ; Shamir, Adi: Visual Cryptography. In: *Advances in Cryptology - EUROCRYPT '94*, Springer-Verlag, 1995, S. 1–12

[11] Pedersen, Torben P.: Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing. In: *Proceedings of the 11th Annual International Cryptology Conference on Advances in Cryptology*, Springer-Verlag, 1992 (CRYPTO '91). – ISBN 3–540–55188–3, S. 129–140

[12] Schneier, Bruce: *Angewandte Kryptographie.* Pearson Studium, 2006. – 83–88, 602–606 S. – ISBN 978–3–8273–7228–3

[13] Shamir, Adi: How to Share a Secret. In: *Communications of the ACM* 22 (1979), Nr. 11, S. 612–613

[14] Simmons, Gustavus J.: How to (Really) Share a Secret. In: *Advances in Cryptology (CRYPTO '88)*, Springer-Verlag, 1990, S. 390–449

Abbildungsverzeichnis

1 Anschauliche Darstellung von Satz 2.1 4

2 Secret Sharing nach Blakley 7

3 Vertraunsnetz bei demokratischem Secret Sharing 12

Die Grafiken wurden vom Autor eigenhändig mit Hilfe der Programme KDE Interactive Geometry (1), GeoGebra (2) und Libre Office Impress (3) erstellt.