Betrugserkennung in Secret Sharing Schemes durch Tests auf Konsistenz

Dissertation

zur Erlangung des Grades
„Doktor der Naturwissenschaften“
am Fachbereich Mathematik
der Justus-Liebig-Universität Gießen

vorgelegt von

Hans-Georg Stambke
aus Recklinghausen

Gießen, 2002

Vorwort

In den letzten Jahren wurde das Papier in vielen Bereichen zugunsten digitaler Dokumente zurückgedrängt. Schriftstücke wie Briefe, Konstruktionspläne, Handbücher, Überweisungsträger und sogar Banknoten befinden sich, was die Papierform angeht, auf dem Rückzug und die elektronischen Pendants nehmen ihren Platz ein. Mit diesem Wandel gehen verschiedene Risiken einher. Für einige dieser Gefahren bietet die vorliegende Arbeit Lösungen an.

Während Papierdokumente durch mehr oder weniger gründlichen Augenschein authentifizierbar und im allgemeinen nur mit hohem Aufwand manipulierbar sind, lassen sich digitale Informationen von jedem Computerbesitzer vervielfältigen und ändern. Das unbemerkte Abfangen, Lesen oder Fälschen fremder Briefe erfordert einen deutlich höheren Aufwand als das Einsehen und Verändern elektronisch übermittelter Daten [SU97].

Authentizität und Vertraulichkeit müssen jedoch keineswegs der Digitalisierung zum Opfer fallen – im Gegenteil. Die Kryptographie kann Geheimnisse sicherer bewahren als jeder Tresor und Fälschungen besser verhindern als eine eigenhändige Unterschrift. Die schon seit Jahrtausenden bekannte Kryptographie entwickelt sich daher derzeit zu einem Fundament der Informationsgesellschaft. Bei Kryptoherstellern dominiert Goldgräberstimmung, während bei Informationsnutzern sowie politischen Weichenstellern Unsicherheit und zum Teil auch Unwissenheit herrschen [Luc97].

Bei der praktischen Anwendung der klassischen Kryptographie ergibt sich eine grundsätzliche Herausforderung. Vor dem gesicherten Nachrichtenaustausch müssen sich die beiden beteiligten Seiten auf einen gemeinsamen Schlüssel einigen – doch auch die Übertragung eines Schlüssels ist eine Nachricht, die abgehört werden könnte. Der Zugriff auf die Schlüssel muss also kontrolliert werden, eine Aufgabe, die zum Key-Management gehört.

Mit der modernen Kryptographie wurden für diese Herausforderung neuartige Antworten gefunden. Im Jahre 1976 veröffentlichten W. Diffie und M. Hellman das Prinzip der Public-Key-Kryptographie [DH76]. Zwei Teilnehmer, die geheim miteinander kommunizieren wollen, brauchen in der Public-Key-Kryptographie (im Gegensatz zur klassischen Kryptographie) kein gemeinsames Geheimnis [BSW01].

Wenig später wollten R. Rivest, A. Shamir und L. Adleman beweisen, dass keine Public-Key-Algorithmen nach dem von W. Diffie und M. Hellman vorgeschlagenen Muster existieren [Beu00]. Sie fanden dabei den ersten Public-Key-Algorithmus, den nach ihnen benannten RSA-Algorithmus [RSA78]. Er ist asymmetrisch, verwendet also zur Ver- und Entschlüsselung zwei verschiedene Schlüssel, einen öffentlichen und einen geheimen. Die beiden Schlüssel werden so konstruiert, dass Botschaften, die mit dem öffentlichen Schlüssel chiffriert wurden, nur mit dem korrespondierenden geheimen Schlüssel wieder

entschlüsselt werden können. Umgekehrt können Nachrichten, die mit dem geheimen Schlüssel chiffriert wurden, nur mit dem entsprechenden öffentlichen Schlüssel entschlüsselt werden. Dadurch kann vom Empfänger sichergestellt werden, dass Nachrichten tatsächlich von dem angegebenen Absender stammen. Dieses Vorgehen ist das digitale Synonym für eine Unterschrift.

In den letzten zwanzig Jahren wurden zahlreiche leistungsfähige Modifikationen des RSA-Algorithmusses vorgestellt und auch in der jüngeren Vergangenheit haben sich verschiedene Mathematiker mit der Forschung auf diesem Gebiet befasst [RS97], [Fia97], [Sch98]. Die wahrscheinlich bekannteste Anwendung des RSA-Algorithmusses ist PGP, ein Programm zur Verschlüsselung von lokalen Dateien und elektronisch übertragenen Nachrichten, sowie zur Verwaltung von Schlüsseln.

In der vorliegenden Arbeit werde ich mich mit einem anderen Verfahren der modernen Kryptographie beschäftigen, den Secret Sharing Schemes. Sie wurden im Jahre 1979 unabhängig von G.R. Blakley [Bla79] und A. Shamir [Sha79] entdeckt. Sie stellen ebenfalls eine Lösung für das angesprochene Key-Management dar. Bei den Secret Sharing Schemes werden Verfügbarkeit und Zugriffssicherheit der Schlüssel dadurch gewährleistet, dass der zu schützende Schlüssel in mehrere Teilgeheimnisse aufgeteilt wird, die anschließend verschiedenen Personen zugeteilt werden. Die Teilgeheimnisse werden so gewählt, dass gewisse, vorher vereinbarte Personengruppen Zugriff auf den geheimen Schlüssel haben, andere nicht.

Die Anzahl der wissenschaftlichen Veröffentlichungen auf dem Gebiet der Secret Sharing Schemes hat in den letzten zehn Jahren deutlich zugenommen. Während G. Simmons [Sim92] im Jahr 1992 eine Bibliographie mit 68 wissenschaftlichen Artikeln zu Secret Sharing Schemes zusammenstellte, fanden D. Stinson und R. Wei [SW98] im Jahr 1998 bereits 216 Veröffentlichungen zu diesem Thema. Diese Tatsache ist einerseits durch den bereits angesprochenen Trend hin zu elektronischen Medien bedingt und zeugt andererseits von der Leistungsfähigkeit der Secret Sharing Schemes.

Die Forschung der letzten Jahre hat sich im wesentlichen mit den folgenden Fragen beschäftigt:

- Wie können Secret Sharing Schemes mathematisch (z.B. geometrisch oder durch Polynome) realisiert werden [Car95], [Gol98], [Ker92], [Sch95], [Kle92], [Sha79], [Bla79]? Einige dieser Realisierungen werden in Kapitel 2.4 vorgestellt.
- Wie groß müssen (bzw. wie klein können) die Teilgeheimnisse eines Secret Sharing Schemes sein [CDV94], [Czi97], [OK98]?
- Wie kann die praktische Anwendung von Secret Sharing Schemes erleichtert werden (z.B. stellt sich die Frage, ob neue Teilgeheimnisse generiert werden können, ohne dass die bisher verteilten ungültig werden) [CGMW97], [Cac96]?
- Welche Eigenschaften haben visuelle Secret Sharing Schemes [NS95], [NS97], [ABDS96], [NP97]? Dabei handelt es sich um Systeme, bei denen Bilder als Teilgeheimnisse an die Teilnehmer verteilt werden, durch deren Überlagerung die vorher bestimmten Teilnehmergruppen das tatsächliche Geheimnis visuell rekon-

struieren können. Bei diesen Systemen ist also keine mathematische Berechnung des geheimen Schlüssels erforderlich.

- Wie kann ein Betrug bzw. ein Betrüger bei der Eingabe der Teilgeheimnisse entdeckt werden [HC96], [Car95], [TW88], [Sim92], [BS91], [MS81], [Neh93]? Secret Sharing Schemes mit dieser Eigenschaft heißen Verifiable Secret Sharing Schemes.
- Kann ein Betrug von Personen entdeckt werden, die keine Teilnehmer sind, die also kein Teilgeheimnis besitzen [Sta96], [Sch99], [YY01]? Secret Sharing Schemes mit dieser Eigenschaft heißen Publicly Verifiable Secret Sharing Schemes.

In der vorliegenden Arbeit werde ich eine Lösung für die letzte der genannten Fragen anbieten. Zwar zeigt die (unvollständige) obige Aufzählung von Veröffentlichungen zu diesem Thema, dass diese Frage bereits eingehend untersucht wurde, jedoch werde ich eine neue und sehr grundlegende Voraussetzung an die mathematische Lösung stellen: Das gefundene Verfahren soll unabhängig von der mathematischen Realisierung des Secret Sharing Schemes sein.

Mit anderen Worten bedeutet das, ich werde ein Rekonstruktionsverfahren für Secret Sharing Schemes entwickeln,

- bei dem die Teilnehmer über die (ohnehin zur Rekonstruktion benötigen) Teilgeheimnisse hinaus keine weiteren Informationen geheim halten müssen, und
- mit dessen Hilfe ein Betrug entdeckt oder Betrüger identifiziert werden kann.

Die grundlegende Idee des Verfahrens beruht darauf, dass dem Secret Sharing Scheme mehr Teilgeheimnisse zur Verfügung gestellt werden, als zur Rekonstruktion des eigentlichen Geheimnisses erforderlich sind. Diese Teilgeheimnisse können untereinander auf Konsistenz untersucht werden.

Für die wichtigsten Secret Sharing Schemes (die Threshold Schemes, die Multilevel Schemes und die Compartment Schemes) wird der praktische Nutzen des Konsistenztests durch die Anwendung auf die jeweilige geometrische Realisierung aufgezeigt. Bei der geometrischen Realisierung eines Secret Sharing Schemes [Ker92] werden den Teilnehmern Punkte in endlichen projektiven Räumen als Teilgeheimnisse zugeordnet. Die Struktur des Secret Sharing Schemes wird durch Wahl der Punkte innerhalb von gewissen linearen Unterräumen abgebildet. Die Rekonstruktion des Geheimnisses erfolgt durch Erzeugnisbildung der beteiligten Teilgeheimnispunkte und Schnitt dieses Erzeugnisses mit einem (öffentlich bekannten) linearen Unterraum.

Für diese geometrischen Realisierungen werde ich Aussagen bezüglich der Vertrauenswürdigkeit des Rekonstruktionsergebnisses und zum Teil auch bezüglich der Ehrlichkeit der einzelnen Teilnehmer ableiten. Der Konsistenztest wird also in der geometrischen Realisierung beweisbar sicher sein.

Eine weitere Stärke meines Konsistenztestes wird darin liegen, dass die Struktur der Teilnehmerkonfiguration analysiert werden kann. Das Secret Sharing Scheme wird mit Hilfe des entwickelten Verfahrens in der Lage sein, alle „minimalen“ berechtigten

Teilmengen der Teilnehmerkonfiguration zu ermitteln. Daraus werden dann Aussagen bezüglich der Kompetenzniveaus der einzelnen Teilnehmer abgeleitet. Während die bisher veröffentlichten Konsistenztests diese Systemgrößen zusätzlich zu den Teilgeheimnissen als Eingabeparameter benötigen [Sim92], [Neh93], wird das hier vorgestellte Verfahren ohne diese Eingaben arbeiten können.

Abschließend noch einige Hinweise, die das Lesen der Arbeit erleichtern werden:

- Die Sätze und Definitionen werden je Kapitel durchnummeriert und bei Querverweisen anhand dieser Nummerierung referenziert. Alle Sätze und Definitionen werden mit einer Absatzmarke  abgeschlossen und so vom umgebenden Text abgegrenzt. Die Absatzmarken werden ausschließlich zu diesem Zweck verwendet.
- Veröffentlichungen werden zitiert, indem die ersten drei Buchstaben des Autorennamens und das Jahr der Publikation genannt werden. Bei Veröffentlichungen von mehreren Autoren werden die Anfangsbuchstaben aller Autoren und das Erscheinungsjahr genannt. Von diesem Verfahren wird nur dann abgewichen, wenn sich für zwei verschiedene Veröffentlichungen dasselbe Kürzel ergeben würde.
- Die meisten Sätze und Definitionen werden nach der mathematischen Formulierung noch einmal in freier Sprache wiedergegeben oder erklärt.

Inhaltsverzeichnis

1. Einleitung

1.1 Verschlüsselung und Schlüsselmanagement

Seit es Sprache gibt, werden Nachrichten ausgetauscht. Seit Nachrichten ausgetauscht werden, gibt es vermutlich das Bestreben, diese Nachrichten einigen Personen zugänglich zu machen, anderen hingegen vorzuenthalten. Es gibt zwei grundsätzliche Möglichkeiten, dieses Problem zu lösen [Beu01], nämlich

- die Existenz der Nachricht geheim halten oder
- die Nachricht verschlüsseln.

Die zweite Möglichkeit wird im folgenden näher betrachtet. Verschlüsselte Nachrichten können von beliebigen Personen gehört, aber nur von berechtigten Teilnehmern entschlüsselt und somit verstanden werden. Dazu chiffriert der Sender einer Botschaft den Klartext *K* mit Hilfe eines (möglicherweise bekannten) Algorithmus *f* unter Verwendung eines *geheimen* Schlüssels *k*. Der Geheimtext *C* wird übermittelt und vom Empfänger mit einem Algorithmus *f'* und einem Schlüssel *k'* zum Klartext entschlüsselt [BR01].

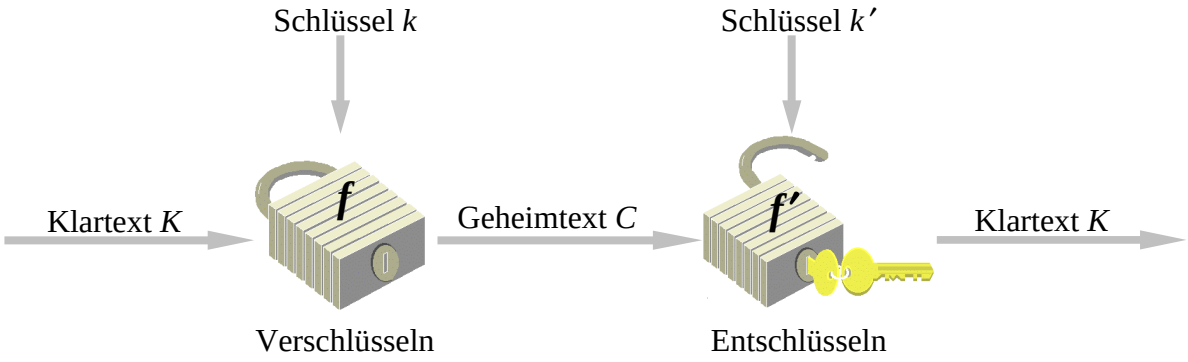


Abbildung 1: Verschlüsselung

Die Sicherheit dieses Verfahrens hängt entscheidend von der Geheimhaltung der Schlüssel ab. Daher ist das Management geheimer Daten ein Grundproblem der praktischen Anwendung von Verschlüsselungsverfahren. Man kann dabei folgende Aspekte unterscheiden:

- Erzeugung,
- Verteilung,
- Speicherung und
- Zerstörung

der geheimen Schlüssel. Diese Aspekte gehören zum Key-Management [BR01].

Beim Key-Management gilt es, zwei zentrale Gesichtspunkte zu berücksichtigen, die sich in der Anwendung häufig widersprechen, nämlich

- Sicherheit und
- Verfügbarkeit.

Erhalten viele Personen von den geheimen Daten Kenntnis, so wächst die Gefahr des Missbrauchs. Die Sicherheit des Systems nimmt folglich ab. Kennen nur wenige Teilnehmer die geheimen Daten, so wird die Verfügbarkeit gefährdet (die Teilnehmer könnten ihr Geheimnis vergessen oder durch Abwesenheit eine Entschlüsselung undurchführbar machen). Für Problemstellungen, bei denen die Systemparameter „Sicherheit der gespeicherten Daten vor unberechtigtem Zugriff“ und „Verfügbarkeit dieser Daten“ vorgebbar sein sollen, eignen sich Secret Sharing Schemes besonders gut.

1.2 Secret Sharing Schemes zur Speicherung geheimer Daten

Bei den Secret Sharing Schemes wird ein geheimer Datensatz so auf eine potentiell große Anzahl von Personen aufgeteilt, dass er nur von bestimmten vorher festgelegten Konfigurationen von Teilnehmern rekonstruiert werden kann [Sim89]. Secret Sharing Schemes bieten so die Möglichkeit, die Verantwortung für sicherheitskritische Prozesse in kontrollierbarer Weise auf mehrere Instanzen zu verteilen. Das Verhältnis zwischen Sicherheit und Verfügbarkeit ist vorgebbar.

Eines der einfachsten Secret Sharing Schemes ist das folgende:
Gegeben sei eine Menge $P = \{P_1, P_2, \ldots, P_n\}$ von n Teilnehmern. Jedem Teilnehmer wird ein Teilgeheimnis aus der Menge $X = \{X_1, X_2, \ldots, X_v\}$ zugeordnet. Das System wird so konstruiert, dass jeweils zwei oder mehr Teilnehmer aus P auf das Geheimnis zugreifen können. Weniger als zwei Teilnehmer bekommen keine Informationen.

Durch die Verteilung des eigentlichen Geheimnisses auf mehrere Personen ergeben sich verschiedene Vorteile [BK95]:

- Die Verantwortung kann in kontrollierbarer Weise auf mehrere Instanzen verteilt werden. Keine Instanz kann allein das Geheimnis abfragen.
- Durch die Möglichkeit, eine Instanz durch eine andere zu ersetzen, ergibt sich eine hohe Ausfallsicherheit (Verfügbarkeit).
- Die Sicherheit von geometrisch realisierten Secret Sharing Schemes ist beweisbar.
- Bei robusten Secret Sharing Schemes (s. Kapitel 1.6) ist eine zentrale Speicherung des zu schützenden Geheimnisses ist nicht erforderlich.

1.3 Anwendungsgebiete für Secret Sharing Schemes

Secret Sharing Schemes werden in verschiedensten Bereichen der Kryptologie eingesetzt. Einige von ihnen werden im folgenden vorgestellt.

1.3.1 Schlüssel-Management bei der Verschlüsselung von Geheimtexten

Bereits in Kapitel 1.1 wurden die verschiedenen Aspekte des Key-Managements aufgezeigt und die Secret Sharing Schemes als praktikable Lösung aufgezeigt. Neben der Verteilung des geheimen Schlüssels auf mehrere Personen sind auch andere Lösungsvarianten denkbar, den Zugriff auf die geheimen Informationen zu kontrollieren. Beispielsweise wurden Schlüsselaustauschprotokolle auf Basis des diskreten Logarithmus entwickelt [DH76].

Diese Protokolle haben jedoch den Nachteil, dass sie nicht beweisbar sicher sind. Einige Secret Sharing Schemes, insbesondere geometrische, besitzen diese beweisbare Sicherheit [Sim92], [Sti92], [Ker92]. Das bedeutet, dass ein Angreifer (der sogar mehrere Teilgeheimnisse kennen darf) nur mit beliebig vorgebbarer Wahrscheinlichkeit das echte Geheimnis raten kann.

1.3.2 Schlüssel-Management bei der Authentikation von Nachrichten

In anderen Anwendungen der Kryptologie steht nicht die Geheimhaltung der Daten im Vordergrund, sondern deren Authentizität. Hier lassen sich wiederum zwei Fragestellungen unterscheiden:

- Sind die Daten so angekommen, wie sie abgeschickt wurden (Nachrichtenauthentikation)?
- Sind die Daten tatsächlich von der Instanz, die als Absender angegeben ist, gesendet worden (Benutzerauthentikation)?

Authentikationssysteme beruhen auf folgendem Verfahren [BR01]:

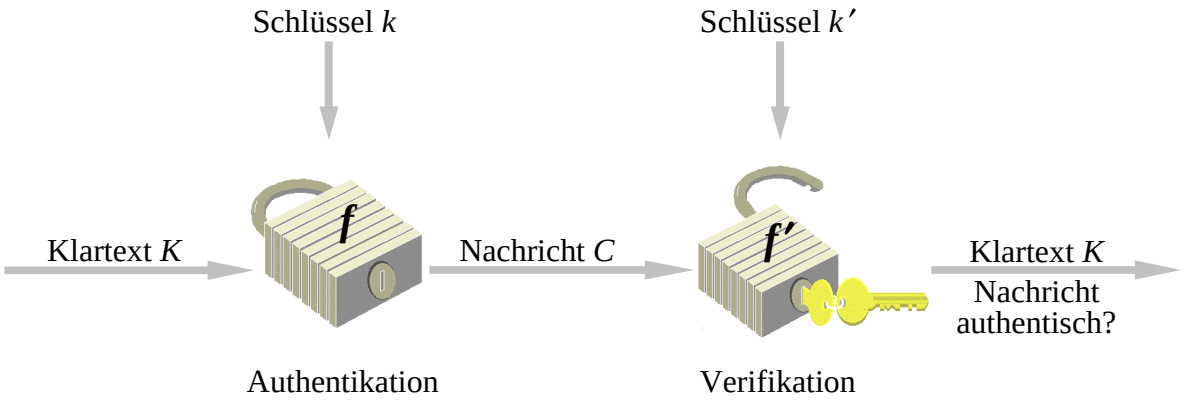


Abbildung 2: Authentikation

Auch bei der Authentikation müssen Schlüssel verwaltet werden. Eine Aufgabe, die mit Secret Sharing Schemes gelöst werden kann.

Im folgenden wird eine spezielle Gruppe von Verfahren zur Nachrichtenauthentikation vorgestellt, nämlich die Verifikationsmethode durch Hinzufügen eines Authentikationscodes (**M**essage **A**uthentication **C**ode, **MAC**) zu der Nachricht. Auf diese Verfahren wird in Kapitel 2.4.3.3 zurückgegriffen.

Bei diesen Verfahren verschlüsselt der Sender seinen Klartext K mit Hilfe eines Schlüssels k und eines Algorithmus f und versendet neben der eigentlichen Nachricht K zusätzlich den verschlüsselten Text $f(K, k)$. Dieser zusätzlich übermittelte, verschlüsselte Text wird Authentikationscode (MAC) genannt.

Ein Angreifer könnte den Klartext K verändern. Da er den Schlüssel k nicht kennt, kann er den zu seiner Nachricht K' passenden $MAC' = f(K', k)$ nur raten.

Der Empfänger kann mit Hilfe des ihm bekannten Schlüssels k und des bekannten Algorithmus f die erhaltene Nachricht K' verschlüsseln und prüfen, ob der übermittelte Klartext authentisch ist.

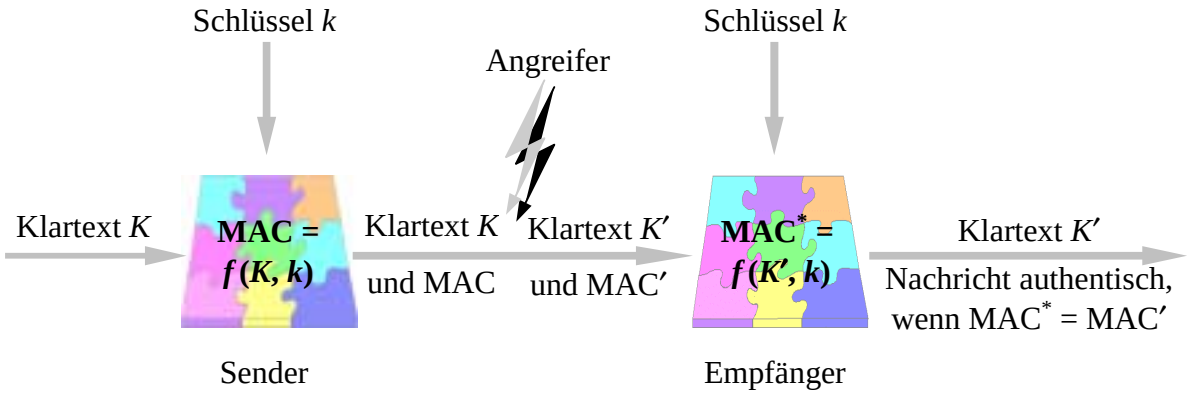


Abbildung 3: Authentikation durch Anhängen eines MAC

1.3.3 Erzeugung elektronischer Kollektiv-Unterschriften

Einige Anwendungen benötigen die Zustimmung mehrerer Personen. So könnte beispielsweise

- eine Tresortür nur von zwei Personen geöffnet werden dürfen oder
- ein Vertrag von mehreren Familienmitgliedern unterschrieben werden müssen.

Sofern die Signatur elektronisch erfolgen kann, stellen auch hier die Secret Sharing Schemes eine Realisierungsmöglichkeit dar. Die Signatur entspricht dem zu schützenden Geheimnis. Sie kann so auf Personen verteilt werden, dass nur Teilnehmerkonfigurationen mit ausreichender Anzahl berechtigter Teilnehmer die Unterschrift leisten können.

1.4 Komponenten eines Secret Sharing Schemes

1.4.1 Lebensphasen eines Secret Sharing Schemes

Vier Lebensphasen eines Secret Sharing Schemes werden unterschieden [BR01].

Definitionsphase

In dieser Phase werden die Anforderungen an das Secret Sharing Scheme festgelegt. Die folgenden Fragen stehen bei der Formulierung dieser Anforderungen im Vordergrund:

- Welche Personen oder Personengruppen dürfen das Geheimnis auslösen?
- Mit welcher Wahrscheinlichkeit soll der Zugriff einer nicht zugelassenen Personengruppe scheitern?

Darüber hinaus können Anforderungen bezüglich der Wahrscheinlichkeit,

- einen Betrüger unter den Teilnehmern zu *bemerken* oder
- einen Betrüger unter den Teilnehmern zu *identifizieren*,

definiert werden.

Mathematische Phase

In dieser Phase müssen mathematische Strukturen gefunden werden, mit denen die formulierten Anforderungen realisiert werden können. Für diese Realisierung haben sich vor allem die projektive Geometrie, die Kombinatorik und die Algebra bewährt.

Geheimniserzeugungsphase

Der Anwender wählt zunächst ein Geheimnis X. Anschließend werden mit den in der mathematischen Phase gefundenen Verfahren die Teilgeheimnisse bestimmt und den einzelnen Teilnehmern zugeteilt.

Die Auswahl des Geheimnisses X muss sowohl von der Formulierung der Anforderungen als auch von der Wahl des mathematischen Modells unabhängig sein.

Anwendungsphase

Schließlich soll das Geheimnis X aus einer legalen Konstellation von Teilgeheimnissen rekonstruiert werden. Nicht legale Gruppen sollen mit der geforderten Wahrscheinlichkeit ein anderes Geheimnis erhalten als X.

In den genannten Lebensphasen des Secret Sharing Schemes sind verschiedene Personen beteiligt. Sie werden in Instanzen aufgeteilt [Kle92].

1.4.2 Instanzen eines Secret Sharing Schemes

Teilnehmer (-instanz)

Jede Person oder Personengruppe, die ein Teilgeheimnis erhält, wird Teilnehmer oder Teilnehmerinstanz genannt. Es wird davon ausgegangen, dass nur Personen, die in einer

legalen Teilnehmerkonstellationen ein Mitwirkungsrecht haben, ein Teilgeheimnis erhalten.

Bewertungsinstanz

Die Person oder Personengruppe, die darüber entscheidet, welche Teilnehmergruppen Zugriff auf das geschützte Geheimnis haben sollen, wird als Bewertungsinstanz bezeichnet. Sie übernimmt alle Aufgaben, die in der Definitionsphase erfüllt werden müssen.

Verteilinstanz (Dealer)

Die Wahl des zu schützenden Geheimnisses *X*, die Erzeugung der erforderlichen Teilgeheimnisse sowie deren Verteilung an die Teilnehmer sind die Aufgaben der Verteilinstanz (siehe Geheimniserzeugungsphase).

Im folgenden wird davon ausgegangen, dass der Dealer integer ist, das heißt

- er betrügt nicht bei der Verteilung der Teilgeheimnisse und
- gibt keine Informationen an Unberechtigte weiter.

Zugriffskontrollinstanz

Während der Anwendungsphase kontrolliert die Zugriffskontrollinstanz (Kontrollinstanz) die Auslösung der zu schützenden Aktion. Eine zulässige Teilnehmerkonstellation erhält das geschützte Geheimnis *X*, unzulässigen Gruppen wird der Zugriff verweigert. Darüber hinaus untersucht die Kontrollinstanz eine Teilnehmergruppe auf das Vorhandensein von Betrügern.

Im folgenden wird davon ausgegangen, dass die Zugriffskontrollinstanz sicher vor unberechtigtem Zugriff ist.

1.5 Betrüger in Secret Sharing Schemes

Bei den bisherigen Betrachtungen in den Kapiteln 1.3 und 1.4 und den genannten Realisierungen wird davon ausgegangen, dass die Teilnehmer beim Rekonstruktionsprozess die Teilgeheimnisse angeben, die ihnen tatsächlich zugeteilt wurden. Es stellt sich die Frage, wie ein Secret Sharing Scheme darauf reagiert, wenn ein Teilnehmer ein falsches Teilgeheimnis angibt, also ein - a priori zufälliges - Teilgeheimnis, das ihm nicht zugeteilt wurde. Ein solcher Teilnehmer wird zunächst naiv *Betrüger* genannt.

Die Gegenwart von Betrügern in einer zulässigen Teilnehmergruppe kann beim Rekonstruktionsprozess folgende Auswirkungen haben:

- Das Secret Sharing Scheme erkennt die Gruppe nicht als zulässig.
- Die Teilnehmergruppe erhält vom Secret Sharing Scheme ein falsches Geheimnis als Antwort.
- Trotz der Gegenwart von Betrügern wird das wahre Geheimnis vom Secret Sharing Scheme rekonstruiert.

Der erste Fall wird dann auftreten, wenn genau die benötigte Anzahl Teilnehmer an der Rekonstruktion teilnimmt, unter den Teilnehmern jedoch ein Betrüger ist. Dann ist die Anzahl der berechtigten Teilnehmer zu gering.

Der zweite Fall ist für die Sicherheit des Systems am gefährlichsten. Der Betrüger erreicht es, dass die Teilnehmergruppe sich von einem falschen Geheimnis überzeugen lässt. Das könnte bedeuten, dass ein falscher Authentikationsschlüssel verwendet oder eine falsche elektronische Unterschrift geleistet wird, ohne dass die Teilnehmer davon Kenntnis haben.

Der dritte Fall wird dann auftreten, wenn zu viele Teilnehmer an der Rekonstruktion teilnehmen und trotz der Betrüger noch hinreichend viele ehrliche Personen in der Teilnehmergruppe sind.

Der zweite der obigen Fälle führt zu den robusten Secret Sharing Schemes.

1.6 Robuste Secret Sharing Schemes

Secret Sharing Schemes heißen robust, wenn sie über eine Zugriffskontrollinstanz verfügen, die nach der Eingabe der Teilgeheimnisse entscheiden kann, ob das berechnete Geheimnis korrekt ist oder nicht.

Die folgende Abbildung zeigt ein robustes Secret Sharing Scheme:

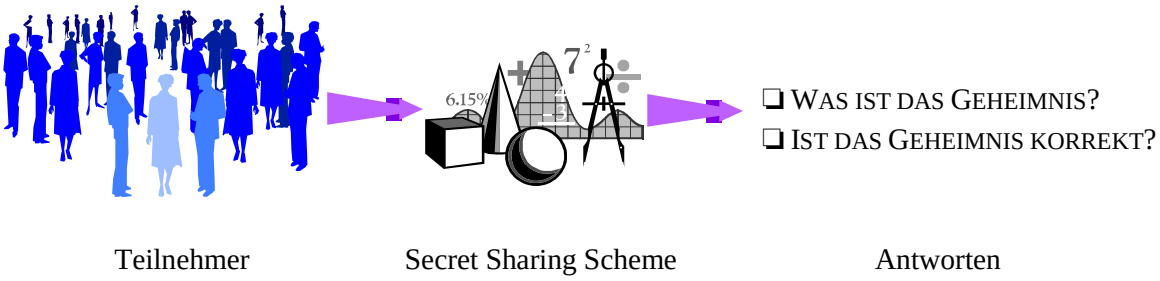


Abbildung 4: Robuste Secret Sharing Schemes

Die Frage nach der Korrektheit eines rekonstruierten Geheimnisses ist dabei schwer zu beantworten, wenn berücksichtigt wird, dass das rekonstruierte Geheimnis nicht mit dem Originalgeheimnis verglichen werden kann. Die zentrale Speicherung des Originalgeheimnisses soll ja gerade durch den Einsatz von Secret Sharing Schemes umgangen werden.

1.7 Zielsetzung

In Kapitel 2 werden grundlegende Modelle und Definitionen vorgestellt, sowie ein Überblick über robuste Secret Sharing Schemes gegeben. Die Secret Sharing Schemes werden zunächst formal definiert. Dazu wird das von A. Kersten [Ker92] vorgestellte Modell zugrunde gelegt. Anschließend wird der Begriff der Perfektheit eingeführt, der für die Beurteilung der Sicherheit von Secret Sharing Schemes eine wesentliche Rolle spielt. Danach werden die wichtigsten Zugriffsstrukturen von Secret Sharing Schemes vorgestellt (die Zugriffsstruktur eines Secret Sharing Schemes beschreibt die Aufteilung von zugriffsberechtigten und nicht zugriffsberechtigten Gruppen von Teilnehmern). Darüber hinaus werden in Kapitel 2 Betrüger in einem Secret Sharing Scheme definiert. Die formale Definition robuster und stark robuster Secret Sharing Schemes bildet den Abschluss der einführenden Grundlagen.

Ziel der Kapitel 3-5 ist es, für die zuvor definierten Zugriffsstrukturen von Secret Sharing Schemes Möglichkeiten und Verfahren zu suchen, mit denen ein Betrug erkannt oder ein Betrüger identifiziert werden kann. Dazu soll dem Secret Sharing Scheme möglichst wenig zusätzliche Information gegeben werden. Insbesondere wird der Zugriffskontrollinstanz keine andere Information als die Teilgeheimnisse der einzelnen Teilnehmern zur Verfügung gestellt.

Die drei folgenden Zugriffsstrukturen werden betrachtet:

- Threshold Schemes,
- Multilevel Schemes und
- Compartment Schemes.

Für diese Zugriffsstrukturen wird ein Test gesucht, mit dessen Hilfe die Zugriffskontrollinstanz allein aufgrund der angegebenen Teilgeheimnisse entscheiden kann, ob das rekonstruierte Geheimnis das tatsächliche ist oder nicht und, sofern möglich, Betrüger identifizieren kann. Dabei wird das Augenmerk hauptsächlich darauf gerichtet, ob und wie der in Kapitel 1.4 als am schwerwiegendsten dargestellte Betrugsfall entdeckt und ein Betrüger identifiziert werden kann.

Es wird gezeigt, dass die beiden anderen Betrugsfälle für die meisten Zugriffsstrukturen kein Problem darstellen, der Betrüger in diesen Fällen allerdings auch nicht als solcher entlarvt werden kann.

2. Grundlagen

2.1 Secret Sharing Schemes

Im folgenden werden die Secret Sharing Schemes formal definiert. Dies geschieht in Anlehnung an die Arbeit von A. Kersten [Ker92].

Zunächst werden die Basismengen definiert, die zur Beschreibung der Secret Sharing Schemes notwendig sind.

2.1 Definition: Basismengen

Seien

$P := \{P_1, P_2, \ldots, P_n\}$	eine Menge von *Teilnehmern*,
$\Gamma \subseteq \mathbf{P}(P)$	eine Menge von Teilmengen der Teilnehmermenge, die *Zugriffsstruktur*,
$K := \{K_0, K_1, \ldots, K_m\}$	eine Menge von möglichen (zu schützenden) *Geheimnissen* (*Keys*),
$X := \{X_1, X_2, \ldots, X_v\}$	eine Menge von *Teilgeheimnissen*, häufig auch als *Shadows* bezeichnet,
$B := \{B_1, B_2, \ldots, B_b\}$	eine Menge von *Blöcken* oder *Indikatoren*.

Anmerkungen zur Definition:

- Jede Person, die ein Teilgeheimnis erhält, ist ein Teilnehmer.
- Die Zugriffsstruktur bezeichnet die Teilnehmermengen, denen der Zugriff auf das geschützte Geheimnis erlaubt ist.
- K_0 bezeichnet das zu schützende Geheimnis.
- Aus den Teilgeheimnissen bildet die Zugriffskontrollinstanz zunächst einen Indikator B_x und rekonstruiert daraus dann das Geheimnis K_x.

Nun werden auf diesen Basismengen Abbildungen definiert, mit deren Hilfe dann die Secret Sharing Schemes definiert werden.

2.2 Definition: BASISABBILDUNGEN

Seien

$$\mathsf{A} \subseteq \left\{ \alpha \subseteq \mathbf{P}(P) \times \mathbf{P}(X) \;\middle|\; \text{für alle } x \subseteq P \text{ ist } \left| \left\{ y \subseteq X \;\middle|\; (x,y) \in \alpha \right\} \right| \leq 1 \right\}$$

eine Menge von Abbildungen von Teilnehmern auf Teilgeheimnisse,

$\beta \subseteq \mathbf{P}(X) \times B$ eine Relation zwischen Mengen von Teilgeheimnissen und Blöcken,

$\kappa : B \to K$ eine Abbildung von Blöcken auf Geheimnisse.

Die folgende Abbildung verdeutlicht den Zusammenhang zwischen den Mengen und Abbildungen:

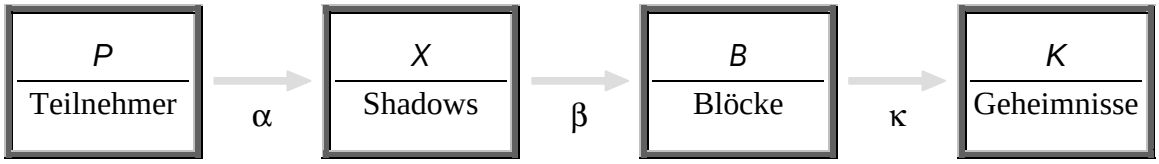


Abbildung 5: Basismengen und -abbildungen eines Secret Sharing Schemes

2.3 Definition: SECRET SHARING SCHEMES

Ein *Secret Sharing Scheme* ist ein Quadrupel (Γ, α, β, κ) mit der Eigenschaft: Für alle $K \in K$ gibt es ein $\alpha_K \in \mathsf{A}$, so dass die beiden folgenden Bedingungen gelten:

S_1: Für alle $G \in \Gamma$ gilt: $\left\{ \kappa(B) \;\middle|\; B \in \mathcal{B} \text{ und } (\alpha_K(G), B) \in \beta \right\} = \{K\}$

S_2: Für alle $H \in \mathbf{P}(P) \setminus \Gamma$ gilt: $\left\{ \kappa(B) \;\middle|\; B \in \mathcal{B} \text{ und } (\alpha_K(G), B) \in \beta \right\} \neq \{K\}$

Jedes $K \in K$ ist ein mögliches Geheimnis. Nach der Definition muss für jedes dieser Geheimnisse eine Abbildung $\alpha_K \in \mathsf{A}$ gefunden werden. Diese Abbildung α_K teilt die Potenzmenge der Teilnehmermenge $\mathbf{P}(P)$ in zwei disjunkte Teilmengen auf:

- Teilnehmermengen, die in der Zugriffsstruktur Γ enthalten sind und das Geheimnis K_0 rekonstruieren können (Bedingung S_1) und
- Teilnehmermengen, die in $\mathbf{P}(P) \setminus \Gamma$ enthalten sind und das Geheimnis K_0 nicht rekonstruieren können (Bedingung S_2).

2.2 Perfektheit

Für die Beurteilung der Sicherheit von Secret Sharing Schemes ist der Begriff der Perfektheit wichtig.

Die Bedingung S_2 aus Definition 2.3 besagt, dass das Secret Sharing Scheme ein beliebiges, von K_0 verschiedenes Geheimnis rekonstruieren soll, wenn eine nicht zulässige Teilnehmerkonfiguration ihre Teilgeheimnisse eingibt. Die Definition lässt offen, mit welcher Wahrscheinlichkeit die verschiedenen $K \neq K_0$ rekonstruiert werden.

Für die Definition der Perfektheit wird zunächst eine Hilfsgröße λ eingeführt.

2.4 Definition:

Sei $Y \in \mathbf{P}(X)$ eine Menge von Teilgeheimnissen. Für alle $K \in \mathcal{K}$ sei

$$\lambda_K(Y) := \left| \left\{ B \in \mathcal{B} \;\middle|\; (Y, B) \in \beta \text{ und } \kappa(B) = K \right\} \right|.$$

Zu einer Menge Y von Teilgeheimnissen und einem beliebigen Geheimnis K gibt $\lambda_K(Y)$ die Anzahl der Blöcke an, die einerseits von Y induziert und andererseits Indikator von K sind. Mit dieser Hilfsgröße kann die Perfektheit definiert werden:

2.5 Definition: PERFEKTHEIT

Ein Secret Sharing Scheme heißt *perfekt*, wenn gilt:
Für alle $H \in \mathbf{P}(\mathcal{P}) \setminus \Gamma$ existiert eine Zahl $\lambda(H)$, so dass für alle $K, K' \in \mathcal{K}$ die Gleichung

$$\lambda_K(H) = \lambda_{K'}(H)$$

gilt.

Ein Secret Sharing Scheme ist also perfekt, wenn für eine unzulässige Konstellation von Teilnehmern alle Geheimnisse aus $\mathcal{K}$ mit der gleichen Wahrscheinlichkeit rekonstruiert werden.

2.3 Wichtige Zugriffsstrukturen

2.3.1 Threshold Schemes

Die einfachste Form eines Secret Sharing Schemes bilden die Threshold Schemes:
Alle Teilnehmergruppen mit einer Mindestanzahl von Teilnehmern sind zulässig - alle Gruppen, die eine geringere Teilnehmerzahl aufweisen, nicht.

2.6 Definition: THRESHOLD SCHEMES

Sei P die Teilnehmermenge eines Secret Sharing Schemes mit $|P| = n$. Ferner sei t eine nicht-negative ganze Zahl mit $t \leq n$. Dann heißt die Zugriffsstruktur $\Gamma \subseteq \mathbf{P}(P)$ mit

$$\Gamma := \left\{ G \in \mathbf{P}(P) \,\middle|\, |G| \geq t \right\}$$

eine (t, n)-*Threshold-Scheme-Zugriffsstruktur*.

Die Definition besagt, dass jedem von n Teilnehmern ein Teilgeheimnis zugeteilt wird, so dass es je t oder mehr Teilnehmern zusammen möglich ist, das Geheimnis zu rekonstruieren.

2.3.2 Multilevel Schemes

Bei den Multilevel Schemes werden den Teilnehmern für die Geheimnisrekonstruktion verschiedene Kompetenzen zugeteilt. Eine Gruppe von Teilnehmern ist dann zulässig, wenn genügend Teilnehmer mit ausreichend hoher Kompetenz teilnehmen. Bei der Rekonstruktion werden Gruppen mit Teilnehmern verschiedener Kompetenzniveaus zugelassen.

2.7 Definition: MULTILEVEL SCHEMES

Sei $P = \{P_1, P_2, \ldots, P_n\}$ die Teilnehmermenge eines Secret Sharing Schemes. Ferner sei $L = \{l_1, l_2, \ldots, l_t\}$ die Menge der Levels mit $l_1 < l_2 < \ldots < l_t$. Jedem Teilnehmer $P \in P$ sei ein Level $l(P) \in L$ zugeordnet. Eine Menge $\Gamma \subseteq \mathbf{P}(P)$ mit

$$\Gamma := \left\{ G \in \mathbf{P}(P) \,\middle|\, \text{es existiert ein } k \in L \text{ mit } \left| \left\{ P \in G \,\middle|\, l(P) \leq k \right\} \right| \geq k \right\}$$

heißt $(l_1, l_2, \ldots, l_t)$-*Multilevel-Scheme-Zugriffsstruktur*.

Für $j = 1, 2, \ldots, t$ seien

$$P^j = \left\{ P \in P \,\middle|\, l(P) \leq l_j \right\}$$

$$\text{und } n_j := |P^j|$$

Die Definition besagt, dass mindestens l_j Teilnehmer des Levels l_j oder eines höherwertigen Niveaus an einer erfolgreichen Rekonstruktion teilnehmen müssen. l_1 ist nach der Definition das Level mit der größten Entscheidungsbefugnis, da die wenigsten Teilnehmer zu Rekonstruktion benötigt werden.

Für die Zugriffsstruktur der Multilevel Schemes werden im folgenden noch die minimalen Levels definiert.

2.8 Definition: MINIMALE LEVELS

Sei $G \in \Gamma$ eine zulässige Teilnehmermenge einer Multilevel-Scheme-Zugriffsstruktur, seien $l_1, l_2, \ldots, l_t$ die Levels.

Ein Level l_i heißt *minimal* in G, wenn

$$l_i = n_i$$

gilt.

Ein Level l_i ist nach obiger Definition genau dann minimal in G, wenn für genau l_i Teilnehmer aus G gilt: $l(P) \leq l_i$.

2.3.3 Compartment Schemes

Die letzte wichtige Klasse von Secret Sharing Schemes, die aufgeführt werden soll, ist die der Compartment Schemes:
Die Teilnehmer werden in disjunkte Klassen eingeteilt. Zur Geheimnisrekonstruktion ist die Zustimmung einer Mindestanzahl von Klassen notwendig. Innerhalb der Klassen ist für die erfolgreiche Ermittlung des Geheimnisses die Teilnahme einer Mindestanzahl von Teilnehmern dieser Klasse erforderlich.

2.9 Definition: COMPARTMENT SCHEMES

Sei $P = \{P_1, P_2, \ldots, P_n\}$ die Teilnehmermenge eines Secret Sharing Schemes und seien $C_1, C_2, \ldots, C_r$ paarweise disjunkte Teilmengen (die *Compartments*) von P mit $P = C_1 \cup C_2 \cup \ldots \cup C_r$.

Seien $t_1, t_2, \ldots, t_r$ natürliche Zahlen mit $2 \leq t_i \leq |C_i|$ für $i = 1, 2, \ldots, r$ und t eine natürliche Zahl mit $t \leq r$. Eine Menge $\Gamma \subseteq \mathbf{P}(P)$ mit

$$\Gamma := \left\{ G \in \mathbf{P}(P) \;\middle|\; \text{es gibt } C_{i_1}, C_{i_2}, \ldots, C_{i_t} \in \{C_1, C_2, \ldots, C_r\} \right.$$
$$\left. \text{mit } |C_{i_j} \cap G| \geq t_{i_j} \text{ für } j = 1, 2, \ldots, t \right\}$$

heißt $(t; t_1, t_2, \ldots, t_r)$-*Compartment-Scheme-Zugriffsstruktur*.

Die Definition besagt, dass für eine erfolgreiche Rekonstruktion des Geheimnisses mindestens t gültige Compartments teilnehmen müssen. Ein Compartment i ist gültig, wenn mindestens t_i Teilnehmer des Compartments ihr Teilgeheimnis einbringen.

Analog zu den minimalen Levels werden minimale Compartments definiert.

2.10 Definition: MINIMALE COMPARTMENTS

Sei $G \in \Gamma$ eine zulässige Teilnehmermenge einer Compartment-Scheme-Zugriffsstruktur, seien $C_1, C_2, \ldots, C_r$ die Compartments.

Ein Compartment $C_i \in \{C_1, C_2, \ldots, C_r\}$ heißt *minimal* in G, wenn

$$\left| C_i \cap G \right| = t_i$$

gilt.

Nach obiger Definition heißt ein Compartment C_i minimal innerhalb einer zulässigen Teilnehmermenge G, wenn genau t_i Teilnehmer dieses Compartments in G enthalten sind.

2.4 Robuste Secret Sharing Schemes

In Kapitel 1.6 wurden robuste Secret Sharing Schemes vorgestellt. Sie werden nun eindeutig definiert.

Robuste Secret Sharing Schemes werden in Umgebungen eingesetzt, in denen die Möglichkeit besteht, dass an der Rekonstruktion beteiligte Personen ein anderes Teilgeheimnis angeben, als ihnen zugeteilt wurde. In dieser Situation kann das rekonstruierte Geheimnis ungleich dem tatsächlichen sein.

Da also Betrüger für die robusten Secret Sharing Schemes eine zentrale Rolle spielen, wird im folgenden zunächst der Begriff des Betrügers formal definiert.

2.4.1 Betrüger

Jeden „Lügner“ - also jeden Teilnehmer, der nicht das ihm zugeteilte Teilgeheimnis angibt - als Betrüger zu bezeichnen, wäre keine hinreichende Definition, denn ein Lügner könnte ein Teilgeheimnis angeben, das einerseits nicht dem entspricht, welches ihm zugeteilt wurde, andererseits aber die Teilnehmergruppe dennoch in die Lage versetzt, das richtige Geheimnis K_0 zu rekonstruieren.

Anmerkung:
Dieser Fall tritt beispielsweise auf, wenn der Lügner das Teilgeheimnis eines anderen Teilnehmers angibt (sofern die Teilnehmerkonstellation mit der Unterstützung dieses anderen Teilnehmers zulässig wäre).

Diese Situation wird aus folgenden Gründen nicht untersucht:

- Das Zugriffskontrollsystem soll die Teilnehmer davor schützen, dass sie einem falschen Geheimnis vertrauen. In der beschriebenen Situation wird jedoch das richtige Geheimnis rekonstruiert.

- Es wird vorausgesetzt, dass der Lügner keine Informationen über die Teilgeheimnisse der anderen Teilnehmer hat. Er kann also das falsche Teilgeheimnis nur zufällig wählen. Die Wahrscheinlichkeit, dass unter diesen Voraussetzungen die oben beschriebene Situation eintritt, kann in der praktischen Anwendung entsprechend klein vorgegeben werden.
- Die Kontrollinstanz soll lediglich dadurch, dass sie mehr Teilgeheimnisse als notwendig erhält, einen Betrug entdecken. Insbesondere soll der Informationsgehalt der Teilgeheimnisse unverändert bleiben. Der beschriebene Angriffsversuch kann unter dieser Voraussetzung nicht entdeckt werden.

Bevor Betrüger in diesem Sinne definiert werden, sollen noch die Begriffe der minimalen Teilnehmerkonstellation sowie der Minimalstruktur einer Teilnehmerkonstellation eingeführt werden.

2.11 Definition: MINIMALE TEILNEHMERMENGEN

Eine zulässige *Teilnehmermenge* $G = \{P_1, P_2, \ldots, P_n\}$ eines Secret Sharing Schemes heißt *minimal*, wenn

$$G \setminus P_i \notin \Gamma \qquad \text{für } i = 1, 2, \ldots, n$$

gilt.

Eine zulässige Teilnehmermenge ist demnach minimal, wenn sie durch Weglassen eines beliebigen Teilnehmers unzulässig wird. In einer zulässigen Teilnehmermenge sind im allgemeinen mehrere minimale Teilnehmermengen enthalten.

2.12 Definition: MINIMALSTRUKTUR EINER TEILNEHMERKONSTELLATION

Sei $G \in \Gamma$ eine zulässige Teilnehmermenge. Die Menge

$$M := \left\{ M \in \mathbf{P}(G) \,\middle|\, M \text{ ist minimal} \right\}$$

heißt *Minimalstruktur einer Teilnehmerkonstellation*.

Die Minimalstruktur enthält also alle minimalen Teilnehmermengen einer zulässigen Teilnehmerkonstellation. Mit Hilfe der Minimalstruktur wird der Betrüger definiert, wie er in der vorliegenden Arbeit untersucht wird.

2.13 Definition: BETRÜGER

Sei $G \in \Gamma$ eine zulässige Teilnehmermenge, M deren Minimalstruktur und K ein zu verschlüsselndes Geheimnis. Ein Teilnehmer P_i aus $G = \{P_1, P_2, \ldots, P_t\}$, der ein Teilgeheimnis $X \neq \alpha_K(P_i)$ angibt, wird genau dann *Betrüger* genannt, wenn

$$\left\{ \kappa(B) \,\middle|\, B \in \mathcal{B} \text{ und } \left(\alpha_K(M), B\right) \in \beta \right\} \neq \{K\}$$

für mindestens ein $M \in \mathcal{M}$ gilt.

Ein Teilnehmer ist also dann ein Betrüger, wenn durch das von ihm angegebene falsche Teilgeheimnis für mindestens eine der minimalen Mengen der betrachteten Teilnehmerkonstellation nicht das tatsächliche Geheimnis *K* rekonstruiert wird.

Anmerkung:
Nach der Definition hängt es von der untersuchten Teilnehmerkonfiguration ab, ob ein „Lügner“ ein Betrüger ist.

2.4.2 Robustheit

Nachdem nun festgelegt ist, wann ein Teilnehmer Betrüger genannt wird, können die robusten Secret Sharing Schemes definiert werden [Sim89].

2.14 Definition: ROBUSTHEIT

Ein Secret Sharing Scheme heißt *robust*, wenn es ein Verfahren gibt, das die Zugriffskontrollinstanz in die Lage versetzt, mit vorgebbarer Wahrscheinlichkeit p zu erkennen, ob in einer Teilnehmerkonstellation ein Betrüger enthalten ist oder nicht.

Die Zugriffskontrollinstanz muss also angeben können, wie hoch die Wahrscheinlichkeit dafür ist, dass das rekonstruierte Geheimnis mit dem tatsächlichen übereinstimmt.

Die Definition lässt das *Identifizieren* des falschen Teilgeheimnisses und damit das Entdecken des Betrügers offen. Daher wird noch der Begriff der starken Robustheit eingeführt.

2.15 Definition: STARKE ROBUSTHEIT

Ein Secret Sharing Scheme verfügt über *starke Robustheit*, wenn es ein Verfahren gibt, das die Zugriffskontrollinstanz in die Lage versetzt, mit vorgebbarer Wahrscheinlichkeit p in einer Teilnehmerkonstellation einen vorhandenen Betrüger zu entdecken.

2.4.3 Beispiele für robuste Secret Sharing Schemes

Die Kontrollinstanz eines robusten Secret Sharing Schemes muss in der Lage sein, die Vertrauenswürdigkeit eines rekonstruierten Geheimnisses K_x mit vorgebbarer Wahrscheinlichkeit zu beurteilen. Zu diesem Zweck kann die Kontrollinstanz jedoch nicht K_x mit dem tatsächlichen Geheimnis K_0 vergleichen. Im folgenden werden einige Realisierungen solcher Secret Sharing Schemes vorgestellt.

2.4.3.1 Methode von M. Tompa und H. Woll

M. Tompa und H. Woll [TW88] haben (t, n)-Threshold Schemes in der Realisierung nach A. Shamir [Sha79] zu robusten Secret Sharing Schemes modifiziert und erweitert. Daher wird die Realisierung nach Shamir zunächst in Kurzform dargestellt.

Das Threshold Scheme wird in GF(q), im Körper der ganzen Zahlen modulo q (q ist eine Primzahl), verwirklicht. In GF(q) ist ein Polynom f vom Grad (t-1) durch t Stützstellen eindeutig bestimmt. Das Polynom lautet allgemein:

$$f(x) = a_0 + a_1 x + \ldots + a_{t-1}\, x^{t-1}$$

Die Koeffizienten $a_0, a_1, \ldots, a_{t-1}$ eines solchen Polynoms aus GF(q) werden zufällig vorgegeben. Das zu schützende Geheimnis K_0 sei der Wert des Polynoms an der Stelle $x = 0$, d. h. $a_0 = K_0$.

Als Teilgeheimnisse werden von der Verteilinstanz die Paare $X_i = (i, f(i))$ für $i = 1, \ldots, n$ ausgegeben. t und mehr Teilnehmer besitzen bei der Rekonstruktion genügend Stützstellen, um das Polynom zu bestimmen und die Zugriffskontrollinstanz kann $a_0 = K_0$ berechnen. Für weniger als t Teilnehmer ist es nicht möglich, Informationen über K_0 vom Secret Sharing Scheme zu erhalten. Das System ist also nach Definition 2.5 perfekt.

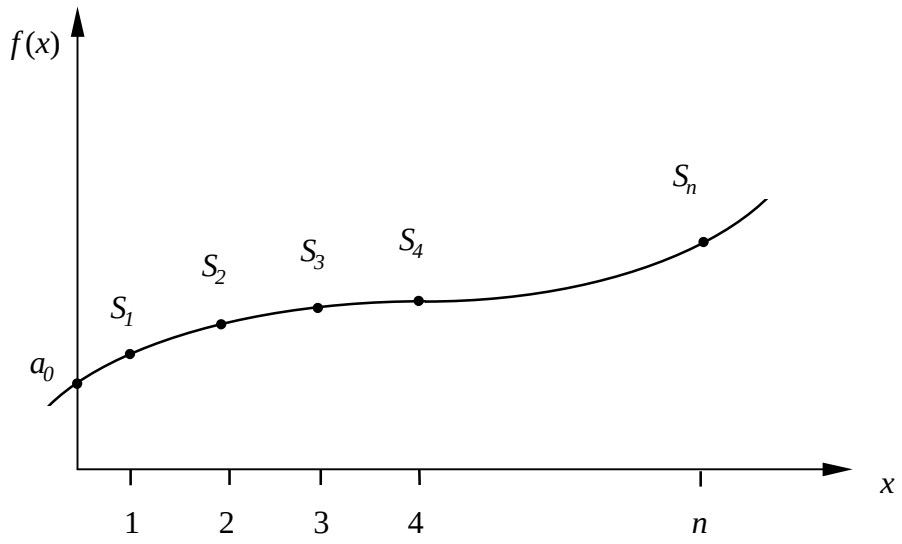


Abbildung 6: Threshold Scheme nach Shamir

M. Tompa und H. Woll haben für dieses Modell gezeigt, dass ein Betrüger, der ein falsches Teilgeheimnis angibt, aus dem rekonstruierten, falschen Geheimnis genügend Informationen erhalten kann, um auf das richtige K_0 schließen zu können. Die ehrlichen Teilnehmer hingegen bemerken den Angriff nicht.

Das Threshold Scheme wird daher wie folgt modifiziert:

- Man wähle zufällige $x_1, x_2, \ldots, x_n$ aus GF(q) und verteile die Paare $X_i = (x_i, f(x_i))$ als Teilgeheimnisse.
- Die Menge der möglichen Geheimnisse $K_T = \{0, 1, 2, \ldots, s\text{-}1\}$ besteht nur aus einer Teilmenge von GF(q).

Die Teilnehmer erhalten umfangreichere Teilgeheimnisse und gleichzeitig werden „gültige“ und „ungültige“ Geheimnisse auf der y-Achse bestimmt. Ein oder mehrere Betrüger sind nicht in der Lage, ihre Teilgeheimnisse so zu wählen, dass im Zusammenspiel mit den ehrlichen Teilnehmern der Schnittpunkt des berechneten Polynoms mit der y-Achse mit einer höheren Wahrscheinlichkeit als

$$p = 1 - \frac{|K_T|}{q} = 1 - \frac{s}{q}$$

in der Menge K_T enthalten ist. Ein Betrug würde also mit der Wahrscheinlichkeit p entdeckt.

Nachteilig für die in Kapitel 1.7 formulierte Zielsetzung ist bei dieser Methode jedoch, dass die Teilnehmer zusätzliche Informationen geheim halten müssen. Ihre Teilgeheimnisse sind umfangreicher geworden.

In [CDV94] wurde gezeigt, dass der Informationsgehalt der Teilgeheimnisse um mindestens

$$\log\left(\frac{1}{\varepsilon}\right)$$

zunehmen muss, wenn ein (t, n)-Threshold Scheme den Betrug einer Gruppe von weniger als t Betrügern mit einer Wahrscheinlichkeit von ε bemerken soll.

2.4.3.2 Einwegfunktionen

Mit Hilfe von Einwegfunktionen ist es möglich, eine Zugriffskontrollinstanz zu entwickeln, die das rekonstruierte Geheimnis K_x mit K_0 vergleichen kann, ohne K_0 zu kennen.

2.16 Definition: EINWEGFUNKTIONEN

Seien X und Y beliebige Mengen. Eine *Einwegfunktion* ist eine umkehrbare Funktion $f: X \rightarrow Y$, so dass $f(x)$ für alle $x \in X$ „leicht“, $f^{-1}(y)$ für alle $y \in Y$ jedoch „schwierig“ zu berechnen ist.

In der Geheimniserzeugungsphase wird (neben der Erzeugung und Verteilung der Teilgeheimnisse) das zu schützende Geheimnis K_0 mit der Einwegfunktion verschlüsselt und der Funktionswert $y_0 := f(K_0)$ gespeichert. Da sich $K_0 = f^{-1}(y_0)$ nach Definition 2.16 nur schwierig berechnen lässt, ist die Forderung für Secret Sharing Schemes, K_0 nicht direkt speichern und vergleichen zu können, erfüllt.

In der Anwendungsphase wird von der Zugriffskontrollinstanz zunächst ein Geheimnis K_x rekonstruiert, anschließend wird $y_x := f(K_x)$ berechnet und geprüft, ob $y_0 = y_x$ gilt. Genau dann, wenn $y_0 = y_x$ erfüllt ist, hat (mit vorgebbarer Wahrscheinlichkeit) kein Betrug stattgefunden.

Bis heute sind jedoch keine Einwegfunktionen gefunden worden, bei denen die „Schwierigkeit“, die Umkehrfunktion zu finden, beweisbar wäre.

2.4.3.3 Prüfungen durch Authentikation

Bereits in Kapitel 1.3.2 wurden die Authentikation und Authentikationscodes vorgestellt. Die Umsetzung einer Kontrollinstanz bei Secret Sharing Schemes mit Hilfe eines Authentikationscodes beruht erneut auf der Idee, K_x mit K_0 zu vergleichen, ohne K_0 zu kennen.

Eine Kontrollinstanz kann mit Hilfe eines Authentikationscodes (MAC) die Überprüfung an zwei Stellen ansetzen.

- **Überprüfen der Eingabe**
  Den Teilnehmern wird neben den eigentlichen Teilgeheimnissen X_i noch der Code $\mathrm{MAC}_{X_i} = f(X_i, S)$ ausgegeben. Wenn die Teilnehmer nun ihr X_i' und MAC_{X_i} eingeben, kann von der Zugriffskontrollinstanz geprüft werden, ob $\mathrm{MAC}_{X_i} = \mathrm{MAC}_{X_i'}$ gilt.
  Anmerkung:
  Mit diesem Verfahren können Betrüger identifiziert werden (starke Robustheit).

- **Überprüfen des rekonstruierten Geheimnisses**
  Entsprechend kann das Geheimnis K_0 verschlüsselt werden und nach der Rekonstruktion wird geprüft, ob $\mathrm{MAC}_{K_0} = \mathrm{MAC}_{K_x}$ gilt.

Bei näherer Betrachtung zeigt sich jedoch, dass dieses Verfahren nicht praktikabel ist. Die Sicherheit hängt nicht, wie es bei den Einwegfunktionen in Kapitel 2.4.3.2 der Fall war, von der mathematischen Schwierigkeit ab, aus MAC_{K_0} das Geheimnis K_0 zu berechnen, sondern von der Geheimhaltung des Authentikationsschlüssels S. Damit befindet man sich wieder am Ausgangspunkt der Secret Sharing Schemes, nämlich der Frage, wie K_0 bzw. S geschützt werden kann.

2.4.3.4 Test auf lineare Konsistenz

Der von G.J. Simmons [Sim92] eingeführte Test auf lineare Konsistenz wurde von R. Nehl [Neh93] näher untersucht. Die Idee bei diesem Test ist, nicht die Menge an Information pro Teilgeheimnis zu erhöhen, sondern die für die Rekonstruktion geforderte Anzahl der Teilgeheimnisse zu steigern, um einen Betrug zu entdecken. Durch die „zu

viel“ eingegebenen Teilgeheimnisse ist es möglich, gewisse Untermengen der Teilgeheimnisse auf Konsistenz zu prüfen.

2.17 Definition: TEST AUF KONSITENZ FÜR SECRET SHARING SCHEMES

Bei einem *Test auf Konsistenz* für Secret Sharing Schemes werden mehrere Untermengen einer Teilnehmermenge, die im Sinne der Definition 2.3 zulässig sind, daraufhin geprüft, ob sie dasselbe Geheimnis rekonstruieren.

Die in [Neh93] vorgestellten Tests auf lineare Konsistenz sind in der Lage, einen Betrug zu erkennen, nicht jedoch den Betrüger zu identifizieren. Als Eingabe benötigen die Secret Sharing Schemes lediglich $t + 1$ Teilgeheimnisse und die Kenndaten der Zugriffsstruktur, d.h.

- bei Threshold Schemes die Schwelle,
- bei Multilevel Schemes die Schwellen der einzelnen Levels und
- bei Compartment Schemes die Schellen in den Compartments sowie die geforderte Mindestanzahl an Compartments.

Ziel der vorliegenden Arbeit ist es, einen Test auf Konsistenz zu entwickeln, der

- als Eingabedaten lediglich Teilgeheimnisse benötigt, und
- über das Erkennen eines Betrugs hinaus auch Betrüger identifizieren kann.

2.4.4 Beispiele für stark robuste Secret Sharing Schemes

2.4.4.1 Supershadows nach E.F. Brickell und D.R. Stinson

Die Methode von E.F. Brickell und D.R. Stinson [BS91] bezieht sich auf (t, n)-Threshold Schemes. Sie realisieren ein nach Definition 2.15 stark robustes Threshold Scheme als Modifikation der geometrischen Realisierung, die von G.R. Blakley [Bla79] erstmals vorgeschlagen wurde.

Sowohl die geometrische Realisierung von G.R. Blakley als auch die Abwandlung von E.F. Brickell und D.R. Stinson werden im folgenden kurz beschrieben.

a) Geometrische Realisierung von G.R. Blakley
Das Threshold Scheme wird in V, einem t-dimensionalen Vektorraum über GF(q) realisiert (q ist eine Primzahl). Die möglichen Geheimnisse liegen auf einer Geraden K, $K_0 \in K$ bezeichnet das zu schützende Geheimnis. Ferner wird in V ein (t-1)-dimensionaler Unterraum B_0 vereinbart, der K nur in K_0 trifft. Aus B_0 wird jedem der n Teilnehmer ein Punkt X_i als Teilgeheimnis zugeteilt. Die Punkte X_i werden zusammen mit K_0 in allgemeiner Lage in B_0 gewählt, d.h. je t Punkte aus $\{K_0, X_1, X_2, \ldots, X_n\}$ erzeugen den t-dimensionalen Unterraum B_0.

Das Threshold Scheme ist für $t = 2$ in der Abbildung dargestellt.

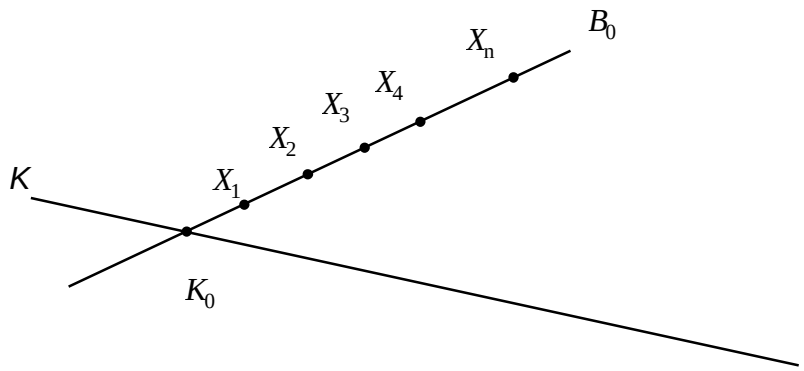


Abbildung 7: Threshold Scheme nach G.R. Blakley

Bei der Rekonstruktion wird das Erzeugnis der eingegebenen Punkte gebildet und mit K geschnitten. Wenn mindestens t Teilnehmer an der Geheimniserzeugung teilgenommen haben, wird die Rekonstruktion K_0 liefern, sonst ist die Schnittmenge leer und die Teilnehmer erhalten kein Geheimnis zurück.

b) Modifikation von Brickell/Stinson

Ein Teilnehmer soll entscheiden können, ob das von einer anderen Person angegebene Teilgeheimnis dem ihr zugeordneten Shadow entspricht oder nicht. Daher erweitern E.F. Brickell und D.R. Stinson das Modell derart, dass jedem Teilnehmer (zusätzlich zu seinem Shadow) Informationen bezüglich der Teilgeheimnisse anderer Teilnehmer zugeteilt werden. An Hand dieser zusätzlichen Informationen kann beurteilt werden, ob ein Teilnehmer betrügt oder nicht. Ein Teilnehmer kann jedoch trotz der zusätzlichen Informationen nicht auf die Teilgeheimnisse der anderen Teilnehmer schließen.

Jedem Teilnehmer werden neben seinem Punkt X_i noch $n - 1$ Unterräume B_{ij}, der Dimension $t - 1$ zugeteilt ($j = 1, 2, \ldots, n - 1$). Die Unterräume sind so gewählt, dass B_{ij} den Shadow des Teilnehmers j enthält.

Die Abbildung zeigt das Modell von Brickell/Stinson für $t = 2$.

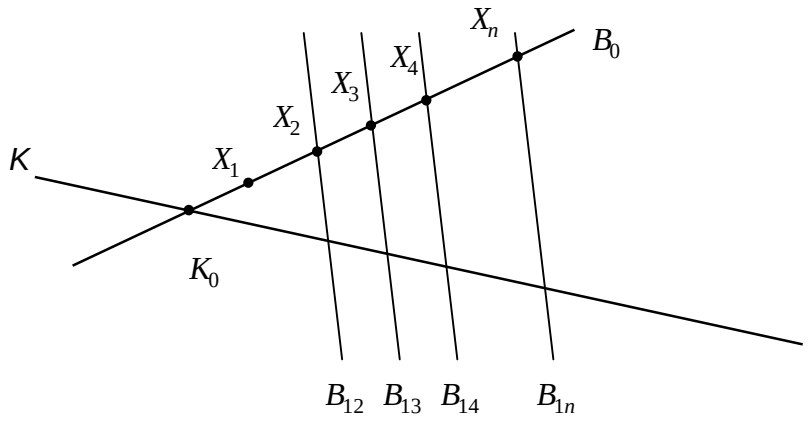


Abbildung 8: Threshold Scheme nach Brickell/Stinson

Anhand der Unterräume, die auch Supershadows genannt werden, kann von einem Teilnehmer P_i mit vorgebbarer Wahrscheinlichkeit kontrolliert werden, ob ein anderer Teilnehmer P_j das ihm zugeordnete Teilgeheimnis angegeben hat, oder nicht. Dazu prüft P_i, ob das von P_j angegebene Teilgeheimnis in B_{ij} liegt. Die Wahrscheinlichkeit lässt sich als

$$p = 1 - \frac{1}{q - 1}$$

bestimmen.

Die beiden wichtigsten Nachteile des Verfahrens sind:

- Das System ist nicht mehr perfekt. Der Teilnehmer i kann die Punkte $K \cap B_{ij}$ auf der Geheimnisgeraden K als Geheimnis K_0 ausschließen ($K \cap B_{ij}$ kann bei entsprechender Wahl der B_{ij} ein einziger Punkt sein).
- Die Teilnehmer müssen für wachsende $|P| = n$ immer größere Teilgeheimnisse sicher aufbewahren.

2.4.4.2 Fehlerkorrektur nach R.J. McEliece und D.V. Sarwate

Die Realisierung von R.J. McEliece und D.V. Sarwate [MS81] verwendet Methoden aus der Codierungstheorie.

Die Codierungstheorie befasst sich damit, Nachrichten, die auf einem unsicheren Kanal übermittelt werden, auf Korrektheit zu überprüfen und eventuelle Fehler zu korrigieren. Die Fehler, die bei der Übermittlung auftreten können, werden als zufällig vorausgesetzt. Der Sender codiert einen Datensatz zu einer Nachricht, übermittelt diese, und der Empfänger decodiert diese Nachricht. Nach dem Entschlüsseln erkennt der Empfänger, ob Fehler bei der Übertragung aufgetreten sind.

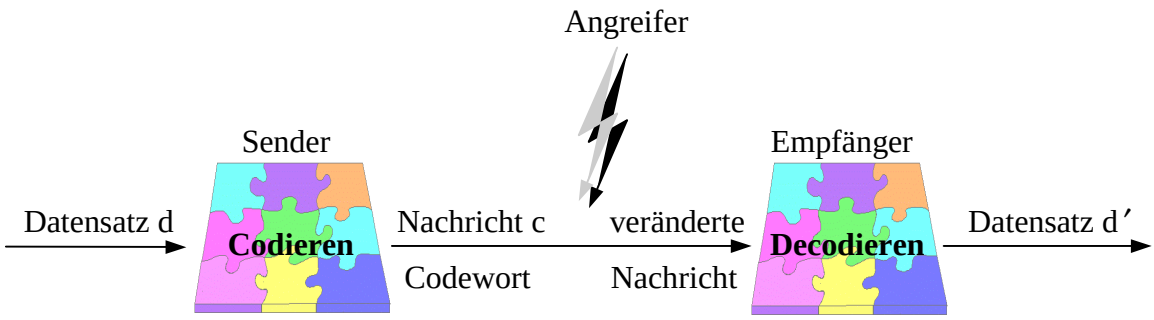


Abbildung 9: Codierung und Decodierung von Daten

Bei „fehlerkorrigierenden Codes“ kann darüber hinaus im allgemeinen der Originaldatensatz trotz des Auftretens von Übertragungsfehlern rekonstruiert werden. Voraussetzung ist, dass die möglichen Nachrichten einen minimalen „Abstand“ zueinander nicht unterschreiten, so dass sich eine durch Übertragungsfehler verfälschte Nachricht in der „Umgebung“ der eigentlichen Nachricht befindet. Genauer gesagt: Ein Code C heißt t-fehlerkorrigierend, wenn der Hamming-Abstand zweier verschiedener Elemente von C mindestens $2t + 1$ ist.

R.J. McEliece und D.V. Sarwate haben einen Zusammenhang zwischen dem Threshold Scheme von Shamir (Vgl. Kapitel 2.4.3.1) und den fehlerkorrigierenden Reed-Solomon Codes aufgezeigt.

Die Idee besteht darin, das ähnlich wie beim Threshold Scheme nach M. Tompa und H. Woll alle möglichen Kombinationen von Teilgeheimnissen in zwei Klassen aufgeteilt werden:

- Kombinationen, die nur durch falsche Angaben mindestens eines Teilnehmers vorkommen können und
- Kombinationen, die mit vorgebbarer Wahrscheinlichkeit ehrlichen Teilnehmern entstammen.

Aus den Teilgeheimnissen $(X_1, X_2, \ldots, X_s)$ wird ein Codewort gebildet. Wenn von den Teilnehmern durch Betrug ein Codewort angegeben wird, dass nicht vorkommen kann, so findet die Kontrollinstanz die Betrüger und kann im allgemeinen auch das richtige Codewort und damit das richtige K_0 rekonstruieren.

Das Verfahren ist λ-fehlerkorrigierend [MS81], wenn für die Anzahl s der zur Verfügung stehenden Teilgeheimnisse gilt:

$$s \geq 2\lambda$$

2.4.4.3 Betrügererkennung nach M. Carpentieri

M. Carpentieri beschreibt eine Realisierung für (t, n)-Threshold Schemes [Car95], die nach Definition 2.5 perfekt ist.

Die Realisierung hat sehr ähnliche Eigenschaften wie ein bereits von T. Rabin und M. Ben-Or beschriebenes Threshold Scheme [RB89], jedoch muss ein Teilnehmer bei Carpentieri weniger Informationen geheim halten: $t + 2(n - 1)$ Elemente eines endlichen Körpers gegenüber $3n - 2$ bei Rabin/Ben-Or.

Die Realisierung von M. Carpentieri basiert auf dem Threshold Scheme von Shamir (vgl. Kapitel 2.4.3.1). Die Teilnehmer erhalten jedoch (ähnlich wie bei Brickell/Stinson) zusätzliche Informationen, mit Hilfe derer sie prüfen können, ob andere Teilnehmer die ihnen zugeordneten Teilgeheimnisse angegeben haben oder nicht.

Das Modell wird über GF(q), dem endlichen Körper mit q Elementen realisiert ($q > n$ ist eine Primzahl). Jeder Teilnehmer P_i bekommt als Teilgeheimnis

- ein t-Tupel $(d_{i_0}, d_{i_1}, \ldots, d_{i_{t-1}})$ sowie
- n-1 Paare (g_{i_j}, b_{i_j}) von Elementen des GF(q) mit $j \neq i$.

Ferner werden $a_1, a_2, \ldots, a_{t-1}$ zufällig in GF(q) gewählt und vor allen Teilnehmern geheim gehalten ($a_1, a_2, \ldots, a_{t-1}$ sind Koeffizienten eines Polynoms, ähnlich wie bei Shamir).

Schließlich sind $\alpha_1, \alpha_2, \ldots, \alpha_n$ verschiedene Elemente aus GF(q) mit $\alpha_1, \alpha_2, \ldots, \alpha_n \neq 0$, die allen Teilnehmern bekannt sind ($\alpha_1, \alpha_2, \ldots, \alpha_n$ sind Stützstellen des Polynoms, ähnlich wie bei Tompa/Woll). Die folgende Abbildung verdeutlicht die Aufteilung der verschiedenen Informationen, die während der Geheimniserzeugungsphase entstehen.

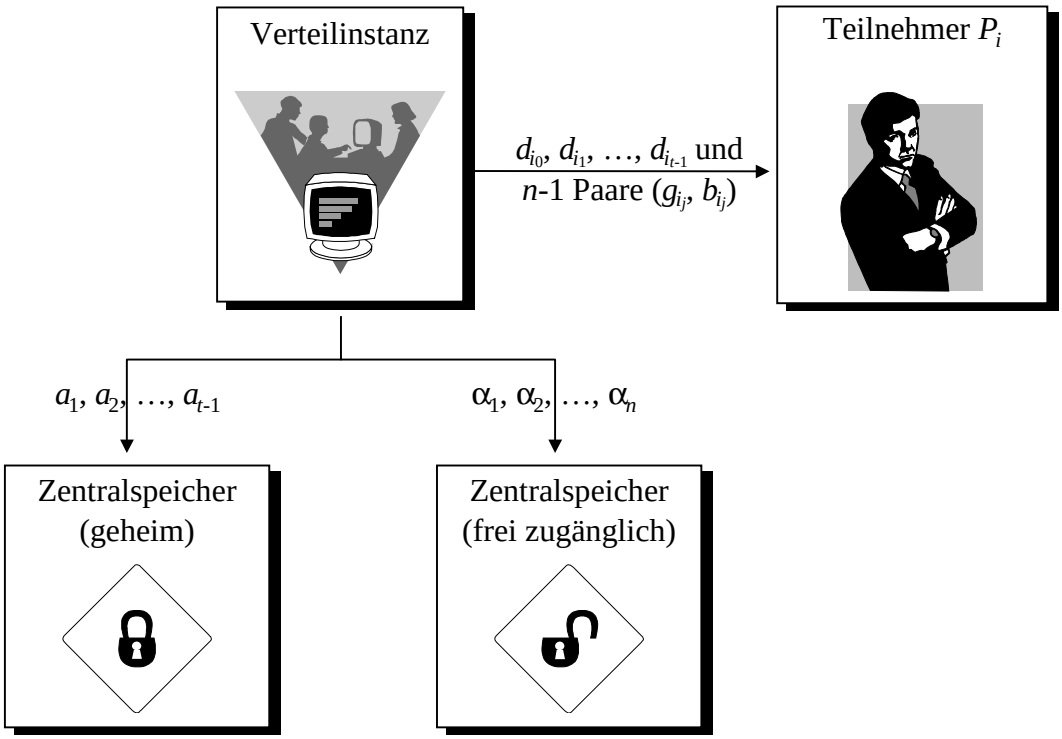


Abbildung 10: Geheimniserzeugungsphase nach M. Carpentieri

Die folgende Tabelle zeigt die Abhängigkeiten der verschiedenen von der Verteilinstanz erzeugten Werte. Sie werden in der aufgeführten Reihenfolge während der Geheimnis-erzeugungsphase gewählt bzw. berechnet.

Wert	Bedingung
K_0	Wählbar
$a_1, a_2, \ldots, a_{t-1}$	Wählbar
$\alpha_1, \alpha_2, \ldots, \alpha_n$	Wählbar
d_{i_0}	$d_{i_0} = f(\alpha_i) = K_0 + a_1\alpha_i + a_2\,\alpha_i^2 + \ldots + a_{t-1}\,\alpha_i^{t-1}$
$d_{i_1}, d_{i_2}, \ldots, d_{i_{t-1}}$	Wählbar
(g_{i_j}, b_{i_j})	$b_{i_j} = g_{i_j}d_{i_0} + \alpha_j d_{i_1} + \alpha_j^2 d_{i_2} + \ldots + \alpha_j^{t-1} d_{i_{t-1}}$

Insgesamt erhält der Teilnehmer P_i:

- d_{i_0}, den Funktionswert des Polynoms an der Stelle α_i, damit t Teilnehmer gemeinsam in der Lage sind, K_0 zu rekonstruieren,
- $d_{i_1}, \ldots, d_{i_{t-1}}$, damit die anderen Teilnehmer das von P_i angegebene Teilgeheimnis überprüfen können und
- $n - 1$ Paare (g_{i_j}, b_{i_j}) damit P_i die Teilgeheimnisse der Teilnehmer P_j überprüfen kann (für $j = 1, 2, \ldots, n$ und $j \neq i$),.

Der Rekonstruktionsprozess während der Anwendungsphase ist in der folgenden Abbildung dargestellt:

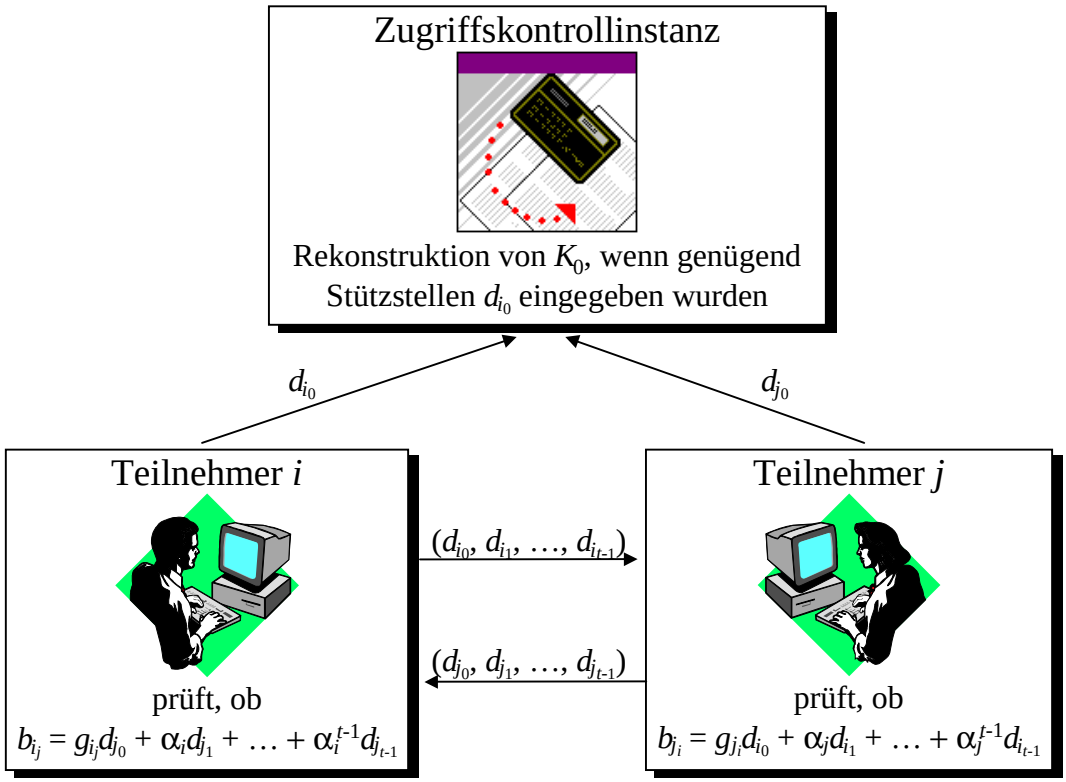


Abbildung 11: Anwendungsphase nach M. Carpentieri

Der Teilnehmer i erhält mit d_{i_0} den Funktionswert des Polynoms f an der Stützstelle α_i. Mit mindestens t dieser Funktionswerte kann das Zugriffskontrollsystem K_0 rekonstruieren. Die Korrektheit des vom Teilnehmer P_j angegebenen Shadows $(y_{j_0}, y_{j_1}, \ldots, y_{j_{t-1}})$ prüft P_i, indem er die Gleichung $b_{i_j} \stackrel{?}{=} g_{i_j} y_{j_0} + \alpha_i y_{j_1} + \alpha_i^2 y_{j_2} + \ldots + \alpha_i^{t-1} y_{j_{t-1}}$ kontrolliert.

Anmerkungen:

- Jeder Teilnehmer erhält an geheimen Informationen ein t-Tupel $d_{i_0}, d_{i_1}, \ldots, d_{i_{t-1}}$, und für jeden der anderen n - 1 Teilnehmer ein Paar (g_{i_j}, b_{i_j}). Er muss $t + 2(n - 1)$ Elemente des Körpers geheim halten.
- Durch die Wahl der Gleichungen $b_{i_j} = g_{i_j} y_{j_0} + \alpha_i y_{j_1} + \alpha_i^2 y_{j_2} + \ldots + \alpha_i^{t-1} y_{j_{t-1}}$ zum Verifizieren der Teilgeheimnisse ist gewährleistet, dass ein Betrug von bis zu t - 1 Betrügern keine Gefahr für das System darstellt. Erst wenn t Betrüger gegenseitig ihre Paare (g_{i_j}, b_{i_j}) offen legen, können sie auf die Teilgeheimnisse der anderen Teilnehmer schließen. Dieser Angriff stellt jedoch keine Gefahr für das System dar, da t Teilnehmer gemeinsam ohnehin Zugriff auf K_0 haben und die geheimen Koeffizienten $a_1, a_2, \ldots, a_{t-1}$ berechnen können.

Die Wahrscheinlichkeit, dass ein Betrüger P_i von einem der ehrlichen Teilnehmer P_j entdeckt wird, ist nach Carpentieri

$$p = 1 - \frac{1}{q\text{-}1}$$

3. Threshold Schemes

3.1 Geometrische Threshold Schemes

Zur Realisierung von Secret Sharing Schemes werden häufig geometrische Modelle benutzt. Sie besitzen hauptsächlich drei Vorteile [Sim92], [BK95]:

- Die Geometrie bietet eine anschauliche und flexible Sprache zur Beschreibung komplexer Zugriffsstrukturen.
- In endlichen projektiven Räumen lässt sich effizient rechnen. Im wesentlichen müssen lineare Gleichungssysteme über einem endlichen Körper gelöst werden. Daher lassen sich geometrische Lösungen sowohl für die Geheimniserzeugungsphase als auch für die Anwendungsphase gut implementieren.
- Geometrische Verfahren sind beweisbar sicher, d.h. eine nicht-zulässige Konstellation von Teilnehmern kann den geheimen Datensatz nur mit einer vorgegebenen Wahrscheinlichkeit erraten.

Im folgenden werden zunächst geometrische Secret Sharing Schemes formal definiert und anschließend die geometrische Realisierung von Threshold Schemes besprochen. Sie wurden bereits in Kapitel 2.4.4.1 durch ein Beispiel angesprochen.

Zunächst wird definiert, wie die Basismengen und -abbildungen, die in den Definitionen 2.1 und 2.2 eingeführt wurden, geometrisch realisiert werden.

3.1 Definition: GEOMETRISCHE SECRET SHARING SCHEMES

Sei $\boldsymbol{P}$ = PG(d,q) der endliche projektive Raum der Dimension d und der Ordnung q. Bei einem *geometrischen Secret Sharing Scheme* [Ker92] sind die Basismengen und Basisabbildungen wie folgt realisiert:

- Die Menge K der möglichen Geheimnisse ist ein s-dimensionaler linearer Unterraum von $\boldsymbol{P}$.
- Die Menge X der Teilgeheimnisse ist die Menge der Punkte von $\boldsymbol{P}$.
- Die Menge B der Indikatorblöcke besteht aus den linearen Unterräumen von $\boldsymbol{P}$, die K jeweils in genau einem Punkt treffen.
- Die Relation β ist für alle $Y \subseteq X$, $B \in B$ definiert durch:
  $(Y, B) \in \beta \Leftrightarrow \langle Y \rangle \leq B$
- Für alle $B \in B$ ist die Abbildung $\kappa : B \rightarrow K$ definiert durch:
  $\kappa(B) := B \cap K$

Anmerkung:
Obige Definition beschreibt die geometrische Realisierung von Secret Sharing Schemes in allgemeiner Form. Die Definition ist unabhängig von der Zugriffsstruktur und muss jeweils für Threshold Schemes, Multilevel Schemes und Compartment Schemes konkretisiert werden. Daher kommen in dieser allgemeinen Definition die Begriffe Teilnehmer und Zugriffsstruktur, wie sie in Definition 2.1 eingeführt wurden, bzw. die Abbildung A (von Teilnehmern auf Teilgeheimnisse) nicht vor.

3.2 Definition: GEOMETRISCHE THRESHOLD SCHEMES

Ein *geometrisches (t, n)-Threshold Scheme* wird als geometrisches Secret Sharing Scheme in PG(d, q) wie in Definition 3.1 realisiert. Für die Dimension d des projektiven Raumes gilt: $d = s + t - 1$.

Ferner sind gegeben:

- $B_0 \in B$ mit $\kappa(B_0) = B_0 \cap K = K_0$ und
- n Punkte von B_0, die zusammen mit K_0 in allgemeiner Lage sind.

Jeder Teilnehmer erhält einen Punkt als Teilgeheimnis. Die Teilgeheimnisse verschiedener Teilnehmer sind unterschiedlich.

Anmerkung:
Jedes geometrische Threshold Scheme ist perfekt [Ker92].

Die folgende Abbildung stellt ein (3, n)-Threshold Scheme für $s = 1$ dar:

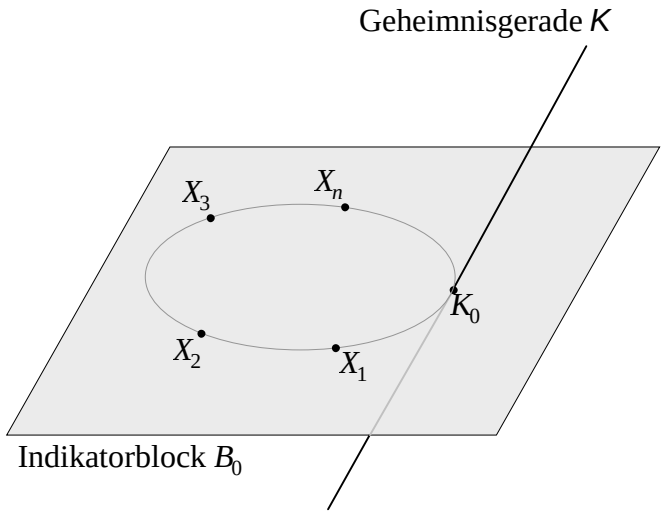


Abbildung 12: Ein geometrisches Threshold Scheme

Finden sich t oder mehr Teilnehmer zusammen, so ist durch die Wahl der Teilgeheimnispunkte in allgemeiner Lage gewährleistet, dass sie den Indikatorblock erzeugen und somit das Geheimnis K_0 rekonstruieren können.

Für weniger als t Teilnehmer sind alle Geheimnisse auf der Geraden K gleichwahrscheinlich, da sie mit ihren Punkten einen Block einer Dimension kleiner als t - 1 erzeugen. Dieser Block schneidet K nicht.

3.2 Erkennen eines Betruges

Die Kontrollinstanz des Threshold Scheme soll nach Eingabe der Teilgeheimnisse entscheiden können, ob das rekonstruierte K_x das tatsächliche Geheimnis ist (bzw. ob einer der eingegebenen Shadows im Sinne der Definition 2.13 von einem Betrüger stammt).

Die zusätzliche Information, die der Zugriffskontrollinstanz des Threshold Schemes zur Lösung dieser Aufgabe bereitgestellt wird, soll lediglich daraus resultieren, dass mehr Teilgeheimnisse, als zur Rekonstruktion erforderlich sind, zur Verfügung stehen.

3.2.1 Test auf Konsistenz

Der von G.J. Simmons [Sim92] vorgestellte Test auf lineare Konsistenz wurde von R. Nehl [Neh93] weiterentwickelt. Hier wird der Test dahingehend erweitert, dass

- Sicherheitsaussagen getroffen und
- Betrüger identifiziert werden können.

Zunächst wird die Kontrollstruktur für Threshold Schemes definiert.

3.3 Definition: KONTROLLSTRUKTUR FÜR THRESHOLD SCHEMES

Sei P die Teilnehmermenge eines Threshold Schemes mit $|P| = n$. Ferner sei t eine nichtnegative ganze Zahl mit $t \leq n$. Dann heißt die Zugriffsstruktur $\Phi \subseteq \mathbf{P}(P)$ mit

$$\Phi := \left\{ F \in \mathbf{P}(P) \;\middle|\; |F| \geq t+1 \right\}$$

eine *(t, n)-Threshold-Scheme-Kontrollstruktur*.

Die in der Kontrollstruktur enthaltenen Teilnehmermengen F heißen *Kontrollmengen*.

Im Vergleich zur Zugriffsstruktur Γ (mit $|G| \geq t$ für alle $G \in \Gamma$) besteht die Kontrollstruktur Φ aus Teilnehmermengen einer Mächtigkeit von mindestens $t + 1$. Zur Zugriffsstruktur des Threshold Schemes wird ein weiteres Teilgeheimnis hinzugefügt, damit es der Zugriffskontrollinstanz möglich ist, mit vorgegebener Wahrscheinlichkeit zu

beurteilen, ob ein Betrüger in einer Teilnehmermenge enthalten ist. Das wird in den Sätzen 3.5 und 3.8 bewiesen.

Beim Test auf Konsistenz wird mit jeder zulässigen Teilmenge G einer Kontrollmenge $F \in \Phi$ die Geheimnisrekonstruktion durchgeführt und geprüft, ob die erhaltenen Ergebnisse übereinstimmen.

3.4 Definition: TEST AUF KONSISTENZ (THRESHOLD SCHEMES)

Seien $F_1, F_2, \ldots, F_f$ Teilmengen einer Kontrollmenge $F \in \Phi$. Die Mächtigkeit der Teilmengen sei t, d.h.

$$f = \binom{|F|}{t}.$$

Für jede Teilmenge F_i ($i = 1, 2, \ldots, f$) werden die Mengen K_i und B_i wie folgt gebildet:

$$B_i := \left\{ B \in \mathcal{B} \middle| \left(\alpha_K(F_i), B\right) \in \beta \right\}$$

$$K_i := \left\{ K \in \mathcal{K} \middle| \kappa(b) = K \text{ für alle } b \in B_i \right\}$$

Die Kontrollmenge F besteht den *Test auf Konsistenz* genau dann, wenn jedes K_i aus genau einem Element besteht und alle diese Elemente gleich sind.

Zur Beantwortung der Frage, ob ein Threshold Scheme durch Anwendung des Tests auf Konsistenz zu einem robusten Secret Sharing Scheme wird, müssen zwei Sachverhalte untersucht werden:

- Bestehen die Kontrollmengen $F \in \Phi$ ohne Betrüger den Test?
- Mit welcher Wahrscheinlichkeit besteht eine Kontrollmenge $F \in \Phi$, die mindestens einen Betrüger enthält, den Test nicht, d.h. mit welcher Wahrscheinlichkeit wird dieser Betrug entdeckt?

Für die weiteren Betrachtungen wird $s = 1$ vorausgesetzt, d.h. der Geheimnisraum $\mathcal{K}$ ist eine Gerade. Nach Definition 3.2 gilt dann für die Dimension d des projektiven Raumes, in dem das Threshold Scheme realisiert wird: $d = t$.

3.5 Satz:

Ein (t, n)-Threshold Scheme sei geometrisch in PG(t, q) wie in Definition 3.2 realisiert. Dann wird der Test auf Konsistenz von einer Kontrollmenge $F \in \Phi$, die keine Betrüger enthält, bestanden.

Beweis:
In dem Test wird jede Teilmenge von F untersucht, die eine Mächtigkeit von genau t besitzt. Da F nur ehrliche Teilnehmer enthält, rekonstruiert das Zugriffskontrollsystem

für jede dieser Untermengen nach den Definitionen 2.3 (Secret Sharing Schemes), 2.6 (Threshold Schemes) und 2.13 (Betrüger) K_0 als Geheimnis.

Alle im Test auf Konsistenz gebildeten Mengen K_i enthalten also genau ein Element und sind gleich. Der Test wird nach Definition 3.4 bestanden.

Im folgenden wird untersucht, wie sich das Vorhandensein eines oder mehrerer Betrüger in einer Kontrollmenge $F \in \Phi$ auf den Test auf Konsistenz auswirkt. Die Abbildung stellt ein (3, n)-Threshold Scheme in der geometrischen Realisierung dar. Unter den Teilnehmern ist ein Betrüger.

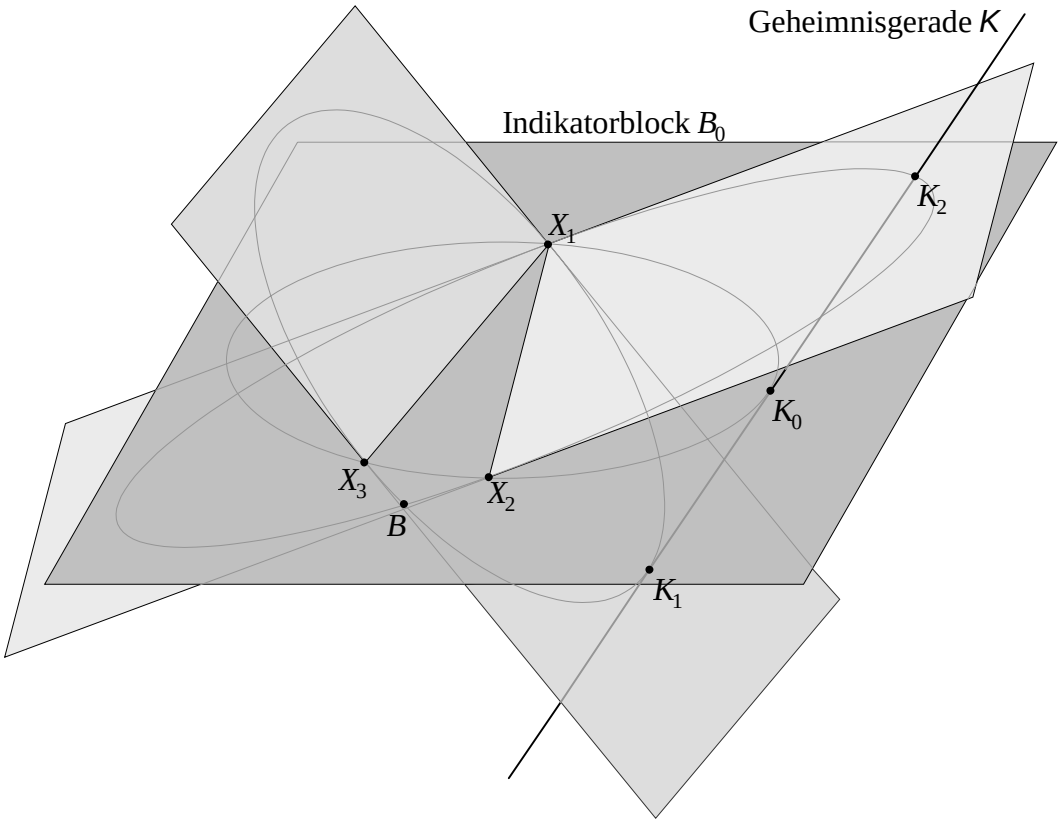


Abbildung 13: Ein (3,n)-Threshold Scheme mit einem Betrüger

Das Teilgeheimnis B stammt von einem Betrüger. Durch Anwesenheit dieses Betrügers werden für alle Untermengen von F, die B enthalten, Geheimnisse ungleich K_0 rekonstruiert. Beispielsweise erhält die Teilmenge $\{X_1, X_3, B\}$ als Geheimnis K_1.

3.6 Satz:

Ein (t, n)-Threshold Scheme sei geometrisch in PG(t, q) wie in Definition 3.2 realisiert. Dann wird der Test auf Konsistenz nach Definition 3.4 von einer Kontrollmenge $F \in \Phi$, die genau einen Betrüger enthält, nicht bestanden, d.h. der Betrug wird entdeckt.

Beweis:
In dem Test wird jede Teilmenge von F untersucht, die eine Mächtigkeit von t besitzt. Da F genau einen Betrüger enthält und nach Definition 3.3 mindestens die Mächtigkeit $t + 1$ hat, müssen mindestens t ehrliche Teilnehmer in F vorhanden sein. Daher gibt es

- mindestens eine Teilmenge der Mächtigkeit t, die *keinen* Betrüger enthält und
- mindestens eine Teilmenge der Mächtigkeit t, die *genau einen* Betrüger enthält.

Für die Teilmenge ohne Betrüger liefert das Zugriffskontrollsystem nach den Definitionen 2.3 (Secret Sharing Schemes) und 2.6 (Threshold Schemes) K_0. Nach Definition 2.13 (Betrüger) wird für die t-elementige Teilmenge mit Betrüger ein $K_x \neq K_0$ rekonstruiert.

Demnach sind mindestens zwei der im Test auf Konsistenz gebildeten Mengen K_i nicht gleich und der Test wird nach Definition 3.4 nicht bestanden.

Sind bei einem (3, n)-Threshold Scheme zwei Betrüger in der Kontrollmenge $F \in \Phi$ enthalten, dann könnte die in Abbildung 14 dargestellte Situation auftreten.

Die Punkte X_1 und X_4 der ehrlichen Teilnehmer liegen mit den Punkten X_2 und X_3 der Betrüger in einer Ebene. Diese Ebene schneidet die Geheimnisgerade in $K_1 \neq K_0$. Die Zugriffskontrollinstanz des (3, n)-Threshold Schemes erkennt den Betrug für $G = \{X_1, X_2, X_3, X_4\}$ nicht. Für diese Situation werden im folgenden Wahrscheinlichkeitsaussagen getroffen.

Anmerkung:
Die Betrachtung dieses Sachverhaltes legt die Frage nahe, wie sich der Test auf Konsistenz verhält, wenn ein einzelner Betrüger seinen Punkt zufällig innerhalb des Indikatorblockes wählt.
Bei dieser Konstellation entdeckt der Test genau dann einen Betrug, wenn die Punkte der Teilnehmer (und des Betrügers), die an der Rekonstruktion beteiligt sind, nicht zusammen mit K_0 in allgemeiner Lage im Indikatorblock sind. Dann gibt es nämlich t-elementige Untermengen von G, die keinen Schnittpunkt mit K haben.
Wenn die Punkte der Teilnehmer zusammen mit dem Punkt des Betrügers und K_0 in allgemeiner Lage sind, wird keine Inkonsistenz festgestellt.
Da nach Definition 2.13 ein Teilnehmer nur dann Betrüger genannt wird, wenn eine der Teilmengen der Kontrollmenge ein Geheimnis ungleich K_0 rekonstruiert, liefert der Test also im Sinne dieser Definition ein korrektes Ergebnis.

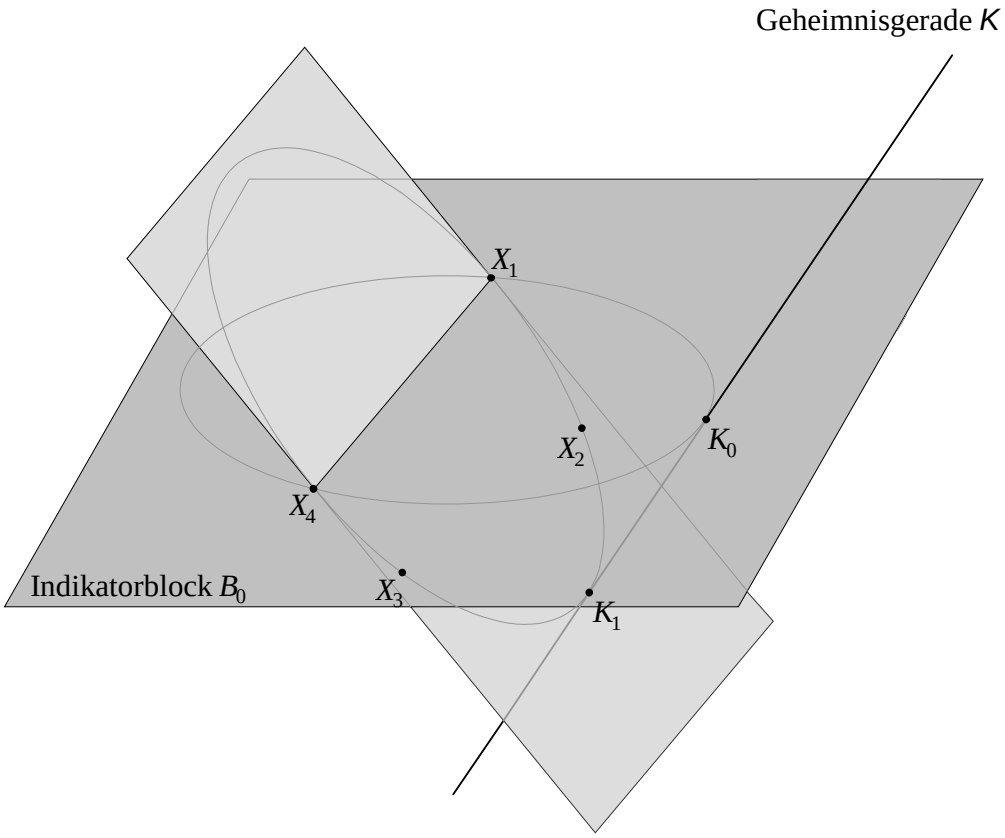


Abbildung 14: Ein (3,*n*)-Threshold Scheme mit zwei Betrügern

Die in Abbildung 14 dargestellte Situation wird näher untersucht. Zunächst wird der Spezialfall „2 Betrüger in einem (*t*, *n*)-Threshold Scheme“ betrachtet.

3.7 Lemma

Ein (*t*, *n*)-Threshold Scheme sei geometrisch in PG(*t*, *q*) wie in Definition 3.2 realisiert. Dann gilt für die Wahrscheinlichkeit p, dass der Betrug zweier Betrüger durch den Test auf Konsistenz nach Definition 3.4 entdeckt wird:

$$p \geq 1 - \frac{q^{t-1} + q^{t-2} + \ldots + q}{q^t + q^{t-1} + \ldots + q^2 - 1}$$

Beweis:
Gezeigt wird:

a) Der Betrug wird mit der Wahrscheinlichkeit p = 1 entdeckt, wenn die Punkte der beiden Betrüger mit den Punkten der ehrlichen Teilnehmer einen Raum der Dimension $d = t$ erzeugen.

b) Für die Wahrscheinlichkeit p′, dass die Betrügerpunkte mit den Punkten der ehrlichen Teilnehmer einen höchstens (t-1)-dimensionalen Raum erzeugen, gilt:

$$p' \leq \frac{q^{t-1} + q^{t-2} + \ldots + q}{q^t + q^{t-1} + \ldots + q^2 - 1}.$$

c) Der Betrug zweier Betrüger wird durch den Test auf Konsistenz mit einer Wahrscheinlichkeit von $p \geq 1 - p'$ entdeckt.

Zu a):
Beim Test auf Konsistenz werden die Rekonstruktionsergebnisse aller t-elementigen Teilmengen der Kontrollmenge $F \in \Phi$ miteinander verglichen. Der Test wird genau dann bestanden, wenn alle Ergebnismengen aus einem Element bestehen und gleich sind.

Wenn die (mindestens t+1) Punkte der Teilnehmer in der Kontrollmenge einen t-dimensionalen Raum aufspannen, dann ist die Geheimnisgerade K ganz in diesem Raum enthalten. Daraus folgt, dass nicht alle Ergebnismengen aus einem Element bestehen und gleich sind. Der Betrug wird entdeckt.

Zu b):
Die (mindestens t-1) Punkte der ehrlichen Teilnehmer erzeugen einen mindestens (t-2)-dimensionalen Raum. Zusammen mit dem Punkt eines der beiden Betrüger wird nach Definition 2.13 ein mindestens (t-1)-dimensionaler Raum aufgespannt. Die gesuchte Wahrscheinlichkeit p′ ist höchstens gleich der Wahrscheinlichkeit, dass der Punkt des anderen Betrügers in diesem (t-1)-dimensionalen Raum liegt.

Dieser Betrüger hat zunächst alle $q^t + q^{t-1} + \ldots + q + 1$ Punkte von PG(t, q) zur Auswahl. Er kann für die Wahl seines Punktes die Geheimnisgerade und sein eigenes Teilgeheimnis, also insgesamt $q + 2$ Punkte, ausschließen. Es bleiben $q^t + q^{t-1} + \ldots + q^2 - 1$ Punkte zur Auswahl.

In dem (t-1)-dimensionalen Unterraum gibt es

$$\frac{q^t - 1}{q - 1} = q^{t-1} + q^{t-2} + \ldots + q + 1$$

Punkte, von denen der Punkt der Geheimnisgerade für den Betrüger nicht in Frage kommt.

Insgesamt ergibt sich also für die gesuchte Wahrscheinlichkeit:

$$p' \leq \frac{q^{t-1} + q^{t-2} + \ldots + q}{q^t + q^{t-1} + \ldots + q^2 - 1}$$

Zu c):
Nach a) wird der Betrug immer entdeckt, wenn die Punkte der Teilnehmermenge durch die Anwesenheit der beiden Betrüger einen t-dimensionalen Raum aufspannen. Nach b) ist die Wahrscheinlichkeit, dass die Punkte einer Teilnehmermenge, die zwei Betrüger

enthält, einen Raum einer Dimension kleiner als t erzeugen, gleich p'. Insgesamt wird also die Anwesenheit der Betrüger mit der Wahrscheinlichkeit $p \geq 1 - p'$ entdeckt, wenn die Betrüger ihre Punkte zufällig wählen.

Für die Gültigkeit des Satzes muss noch gezeigt werden, dass die beiden Betrüger diese Wahrscheinlichkeit p auch durch Absprache untereinander nicht reduzieren können.

Die Betrüger kennen die Geheimnisgerade und ihre beiden Punkte. Diese Information reicht nicht aus, durch geschickte Wahl der beiden Betrügerpunkte die Dimension des Erzeugnisses aller Teilnehmerpunkte zu reduzieren. Die beiden Betrüger spannen mit ihren Punkten einen mindestens 1-dimensionalen Raum auf, zusammen mit den t-1 ehrlichen Teilnehmern erzeugen sie mit mindestens der unter b) errechneten Wahrscheinlichkeit einen t-dimensionalen Raum.

Anmerkungen:

- Für Kontrollmengen einer Mächtigkeit von mehr als $t + 1$ ist die Wahrscheinlichkeit des Entdeckens zweier Betrüger gleich 1. Die mindestens t ehrlichen Teilnehmer, die dann in der Kontrollmenge enthalten sind, erzeugen bereits einen (t-1)-dimensionalen Unterraum. Die Betrügerpunkte können nach Definition 2.13 nicht in allgemeiner Lage mit den anderen Punkten in diesem Unterraum liegen.
- Für die Erfolgswahrscheinlichkeit eines Betruges gilt:

$$\lim_{q \to \infty} p' = \frac{1}{q + 1}$$

Nach diesen Überlegungen wird nun die Wahrscheinlichkeit ermittelt, den Betrug beliebig vieler Teilnehmer durch den Test auf Konsistenz zu entdecken.

3.8 Satz:

Ein (t, n)-Threshold Scheme sei geometrisch in PG(t, q) wie in Definition 3.2 realisiert. Dann gilt für die Wahrscheinlichkeit p, dass der Betrug von x Betrügern ($x < t$), die sich untereinander nicht absprechen, durch den Test auf Konsistenz nach Definition 3.4 entdeckt wird:

$$p \geq 1 - \frac{q^{t-1} + 2q^{t-2} + \ldots (t-3)q^3 + (t-2)q^2 + (t-2)q}{q^t + q^{t-1} + \ldots + q^2 - 1}.$$

Beweis:
Der Beweis erfolgt analog zum Beweis von Lemma 3.7. Gezeigt wird:

a) Der Betrug wird mit der Wahrscheinlichkeit $p = 1$ entdeckt, wenn die Punkte der Betrüger mit den Punkten der ehrlichen Teilnehmer einen Raum der Dimension $d = t$ aufspannen.

b) Für die Wahrscheinlichkeit p′, dass die Betrügerpunkte mit den Punkten der ehrlichen Teilnehmer einen höchstens (t-1)-dimensionalen Raum erzeugen, gilt:

$$p' \leq \frac{q^{t-1} + 2q^{t-2} + \ldots (t-3)q^3 + (t-2)q^2 + (t-2)q}{q^t + q^{t-1} + \ldots + q^2 - 1}.$$

Zu a):
Die Aussage folgt aus dem Beweis zu a) von Lemma 3.7.

Zu b):
Die Wahrscheinlichkeiten dafür, dass jeweils einer der Betrüger seinen Punkt so wählt, dass die Dimension des Erzeugnisses aller Teilnehmerpunkte reduziert wird, werden addiert. Die Betrüger werden sukzessiv zu der Teilnehmermenge hinzugefügt und die Wahrscheinlichkeit für einen erfolgreichen Betrug ermittelt.

Der ungünstigste Fall für den Test auf Konsistenz wird betrachtet:
- Anwesenheit von t - 1 Betrügern
- in einer Kontrollmenge der Mächtigkeit t + 1.

Jeder Betrüger hat

$$Q := q^t + q^{t-1} + \ldots + q^2 - 1$$

Punkte zur Auswahl (alle Punkte von PG(t, q), abzüglich der Geheimnisgeraden K und des eigenen Teilgeheimnisses). Die Punkte der Betrüger seien X_1, X_2, …, X_{t-1}.

Die (mindestens zwei) ehrlichen Teilnehmer spannen einen mindestens 1-dimensionalen Unterraum auf. X_1 muss als Betrüger nach Definition 2.13 seinen Punkt außerhalb der Indikatorebene wählen und kann ihn daher nicht innerhalb des von den ehrlichen Teilnehmern erzeugten Raumes wählen. Durch seine Anwesenheit allein kann der Test also nicht scheitern (diese Aussage folgt auch aus Satz 3.6).

Der Test scheitert, wenn der zweite Betrüger seinen Punkt in der Ebene wählt, welche X_1 zusammen mit den ehrlichen Teilnehmer aufspannt. Die Wahrscheinlichkeit dafür ist

$$p_2 := \frac{q^2 + q}{Q}.$$

Die Wahrscheinlichkeit, dass der Teilnehmer X_i seinen Punkt in dem i-dimensionalen Unterraum wählt, den seine Vorgänger mit den ehrlichen Teilnehmern aufspannen, ist

$$p_i := \frac{q^i + q^{i-1} + \ldots + q}{Q}.$$

Die Wahrscheinlichkeit für das Scheitern des Tests bei Anwesenheit von t - 1 Betrügern ist

$$p' \leq \sum_{i=2}^{t-1} p_i = \frac{q^{t-1} + 2q^{t-2} + \ldots (t-3)q^3 + (t-2)q^2 + (t-2)q}{q^t + q^{t-1} + \ldots + q^2 - 1}$$

Die Wahrscheinlichkeit für den Erfolg des Testes ist für eine beliebige Anzahl von Betrügern

$$p \geq 1 - p'.$$

Aus a) und b) folgt die Aussage des Satzes für zufällig gewählte Betrügerpunkte.

Anmerkung:
Die Möglichkeit, dass die Betrüger sich untereinander absprechen, muss ausgeschlossen werden. Die x Betrüger können für $x \geq 3$ ihre Punkte auf einer Geraden wählen, die K in K_x schneidet. Dann sind in jeder t-elementigen Untermenge einer Kontrollmenge der Mächtigkeit t+1 mindestens zwei Betrüger und höchstens t-2 ehrliche Teilnehmer enthalten. Jeder dieser t-elementigen Untermengen rekonstruiert dann K_x und der Betrug wird nicht entdeckt.

Interessant an der Aussage des Satzes 3.8 ist, dass sich wie in Lemma 3.7 für große q eine Erfolgswahrscheinlichkeit für einen Betrug von

$$\lim_{q \to \infty} p' = \frac{1}{q+1}$$

ergibt. Die Anzahl x der Betrüger in einem (t, n)-Threshold Scheme hat demzufolge für $1 < x < t$ und $q \to \infty$ keinen Einfluss auf die Wahrscheinlichkeit, dass ein Betrug durch den Test auf Konsistenz entdeckt wird.

Nach Satz 3.8 ist eine Zugriffskontrollinstanz durch den mit Definition 3.4 eingeführten Test auf Konsistenz in der Lage, einen Betrug mit vorgebbarer Wahrscheinlichkeit zu erkennen. Insoweit ist ein Teil der in Kapitel 1.7 genannten Zielsetzung erfüllt.

Bei genauer Betrachtung des Testes auf Konsistenz fällt jedoch auf, dass die Zugriffskontrollinstanz eine Information braucht, die nicht den Teilgeheimnissen entnommen werden kann. Für das Bilden der t-elementigen Untermengen wird die Schwelle t des Threshold Schemes benötigt. Das ist nach der in Kapitel 1.7 formulierten Zielsetzung nicht gewünscht.

Im folgenden wird ein Test auf Konsistenz durch minimale Mengen definiert, der dieser Zielsetzung entspricht.

3.2.2 Test auf Konsistenz durch minimale Mengen

Die Minimalstruktur einer Teilnehmermenge wurde durch Definition 2.12 eingeführt. Sie enthält alle minimalen Mengen einer zulässigen Teilnehmermenge. Mit dieser Minimalstruktur wird ein Test auf Konsistenz definiert.

3.9 Definition: TEST AUF KONSISTENZ DURCH MINIMALE MENGEN

Sei $G \in \Gamma$ eine zulässige Teilnehmermenge. Seien $M_1, M_2, \ldots, M_m$ die Teilmengen der Minimalstruktur M von G mit $m = |M| > 1$.

Für jede der Teilmengen M_i werden die Mengen B_i und K_i wie folgt gebildet:

$$B_i := \left\{ B \in \mathcal{B} \;\middle|\; \left(\alpha_K(M_i), B \right) \in \beta \right\}$$

$$K_i := \left\{ K \in \mathcal{K} \;\middle|\; \kappa(b) = K \text{ für alle } b \in B_i \right\}$$

Die Menge G besteht den *Test auf Konsistenz durch minimale Mengen* genau dann, wenn jedes K_i aus genau einem Element besteht und alle diese Elemente gleich sind.

Anmerkung:
Wenn unter den Teilnehmern kein Betrüger ist, dann entspricht die Minimalstruktur M der Kontrollstruktur Φ aus Definition 3.3.

3.10 Satz:

Ein (t, n)-Threshold Scheme sei geometrisch in PG(t, q) wie in Definition 3.2 realisiert. Ferner sei eine Teilnehmermenge $G \in \Gamma$ einer Mächtigkeit von mindestens $t + 1$, die keine Betrüger enthält, gegeben.

Dann wird der Test auf Konsistenz durch minimale Mengen nach Definition 3.9 bestanden.

Beweis:

a) Prüfen der Voraussetzung des Testes: $|M| \stackrel{?}{>} 1$

Die Punkte der mindestens $t + 1$ Teilnehmer sind nach Definition 3.2 zusammen mit K_0 in allgemeiner Lage im Indikatorblock. Da der Indikatorblock (t-1)-dimensional ist, besteht die Minimalstruktur nach Definition 2.12 genau aus allen t-elementigen Teilmengen von G.

Das sind (mit $t > 1$)

$$\binom{t+1}{t} = t+1 > 1$$

Stück.

b) Ergebnis des Testes:

Da unter den Teilnehmern keine Betrüger sind, rekonstruiert die Zugriffskontrollinstanz für jede dieser *t*-elementigen Teilmengen dasselbe Geheimnis. Der Test auf Konsistenz durch minimale Mengen wird nach Definition 3.9 bestanden.

3.11 Satz:

Ein (*t*, *n*)-Threshold Scheme sei geometrisch in PG(*t*, *q*) wie in Definition 3.2 realisiert. Ferner sei eine Teilnehmermenge einer Mächtigkeit von mindestens $t + 1$ gegeben. Sie enthalte *x* Betrüger ($x < t$), die sich untereinander nicht absprechen.

Dann gilt für die Wahrscheinlichkeit p, dass der Betrug durch den Test auf Konsistenz durch minimale Mengen nach Definition 3.9 entdeckt wird:

$$p \geq 1 - \frac{q^{t-1} + 2q^{t-2} + \ldots (t-3)q^3 + (t-2)q^2 + (t-2)q}{q^t + q^{t-1} + \ldots + q^2 - 1}$$

Beweis:
Der Beweis erfolgt analog zum Beweis von Satz 3.8. Gezeigt wird:

a) Der Betrug wird mit der Wahrscheinlichkeit $p = 1$ entdeckt, wenn die Punkte der Betrüger mit den Punkten der ehrlichen Teilnehmer einen Raum der Dimension $d = t$ aufspannen.

b) Für die Wahrscheinlichkeit p′, dass die Betrügerpunkte mit den Punkten der ehrlichen Teilnehmer einen höchstens (*t*-1)-dimensionalen Raum erzeugen, gilt:

$$p' \leq \frac{q^{t-1} + 2q^{t-2} + \ldots (t-3)q^3 + (t-2)q^2 + (t-2)q}{q^t + q^{t-1} + \ldots + q^2 - 1}.$$

Zu a):
Die mindestens $t + 1$ Teilnehmer erzeugen durch die Anwesenheit von Betrügern einen *t*-dimensionalen Raum. Da in diesem Raum die gesamte Geheimnisgerade enthalten ist, folgt mit Definition 2.11:

- Es gibt mehrere minimale Mengen der Mächtigkeit *t* (die Voraussetzung des Tests ist erfüllt) und
- mindestens zwei der minimalen Mengen haben unterschiedliche Schnittpunkte mit der Geheimnisgeraden.

Der Test wird folglich nicht bestanden.

Zu b):
Die Wahrscheinlichkeit p′ wurde bereits im Beweis zu Satz 3.8 ermittelt.

Insgesamt folgt die Aussage des Satzes.

Anmerkung:
Wie in Satz 3.8 muss auch hier ausgeschlossen werden, dass die Betrüger sich untereinander absprechen. Die Betrüger können, genau so wie in der Anmerkung zu Satz 3.8 beschrieben, durch Absprache die Dimension des von allen Teilnehmerpunkten erzeugten Raumes reduzieren und damit die Zugriffskontrollinstanz täuschen.

Aus Satz 3.11 folgt, dass die beiden Tests auf Konsistenz nach den Definitionen 3.4 und 3.9 unter denselben Voraussetzungen einen Betrug entdecken. Dem Vorteil, dass einer Zugriffskontrollinstanz beim Test auf Konsistenz durch minimale Mengen die Schwelle nicht bekannt sein muss, stehen also keine wesentlichen Nachteile gegenüber.

3.3 Finden eines Betrügers

Bei den im vorhergehenden Abschnitt definierten Tests auf Konsistenz zum Entdecken eines Betruges können zwei Situationen auftreten:

- Alle (mindestens $t + 1$) Punkte liegen in einem ($t - 1$)-dimensionalen Unterraum in allgemeiner Lage. In diesem Fall hat mit vorgebbarer Wahrscheinlichkeit *kein* Betrug stattgefunden.
- Die Punkte der mindestens $t + 1$ Teilnehmer spannen einen t-dimensionalen Raum auf. In diesem Fall hat mit Sicherheit ein Betrug stattgefunden.

Zum Identifizieren der Betrüger müssen die Punkte gefunden werden, die sich nicht im Indikatorblock befinden oder innerhalb des Indikatorblockes nicht in allgemeiner Lage sind. Mit Hilfe des in der nächsten Definition eingeführten Tests auf Konsistenz wird die Zugriffskontrollinstanz in der Lage sein, eben diese Punkte zu finden.

Die Idee zu diesem Test beruht auf folgender Beobachtung:
Wenn in einer Teilnehmermenge mindestens $t + 1$ ehrliche Teilnehmer enthalten sind, dann wird durch die beiden Tests auf Konsistenz (Definitionen 3.4 und 3.9) das tatsächliche Geheimnis K_0 mindestens ($t + 1$)-mal rekonstruiert. Wenn diese Mehrfachrekonstruktion eines Punktes der Geheimnisgeraden für minimale Mengen, die Betrüger enthalten, mit vorgebbarer Wahrscheinlichkeit ausgeschlossen werden kann, dann können die Betrüger identifiziert werden (das wird in Satz 3.18 bewiesen).

3.12 Definition: ERWEITERTER TEST AUF KONSISTENZ (THRESHOLD SCHEMES)

Sei $G \in \Gamma$ eine zulässige Teilnehmermenge. Seien $M_1, M_2, \ldots, M_m$ die Teilmengen der Minimalstruktur M von G nach Definition 2.12.

Für jede der Teilmengen M_i werden die Mengen B_i und K_i wie folgt gebildet:

$$B_i := \left\{ B \in \mathcal{B} \middle| \left(\alpha_K(M_i), B \right) \in \beta \right\}$$

$$K_i := \left\{ K \in \mathcal{K} \middle| \kappa(b) = K \text{ für alle } b \in B_i \right\}$$

Ferner ist $\mathcal{D}$ die *Durchschnittmenge* mit

$$\mathcal{D} = \left\{ K \in \mathcal{K} \middle| K \in K_i, K_j \ (i \neq j) \right\}.$$

Der *erweiterte Test auf Konsistenz* ist *durchführbar*, wenn

$$\mathcal{D} \neq \{\ \}.$$

Die Menge *G besteht* den *erweiterten Test auf Konsistenz* genau dann, wenn jedes K_i aus genau einem Element besteht und alle diese Elemente gleich sind.

Besteht die Menge den Test nicht, so werden zwei *Ergebnismengen* gebildet:

$$\mathcal{E}_E := \left\{ P \in G \middle| \text{ es existiert ein } i \text{ mit } P \in M_i \text{ und } K_i \subseteq \mathcal{D} \right\}$$

$$\mathcal{E}_B := G \setminus \mathcal{E}_E$$

Nach obiger Definition sind für den Test auf Konsistenz folgende Schritte durchzuführen:

- Für jede minimale Menge M_i wird die Rekonstruktion durchgeführt. Daraus ergeben sich die Mengen K_i.
- Die Durchschnittmenge $\mathcal{D}$ enthält alle $K \in \mathcal{K}$, die in mindestens zwei der Mengen K_i enthalten sind. In $\mathcal{D}$ sind also alle Punkte der Geheimnisgeraden enthalten, die von mindestens zwei verschiedenen minimalen Mengen rekonstruiert werden.
- Der Test ist durchführbar, wenn mindestens ein Punkt der Geheimnisgeraden mehrfach rekonstruiert wurde (d.h. $\mathcal{D} \neq \{\ \}$).
- Der Test wird bestanden, wenn alle K_i einelementig und gleich sind.
- Die Ergebnismenge $\mathcal{E}_E$ enthält einen Teilnehmer *P*, wenn *P* in einer minimalen Menge M_i enthalten ist, die ein K_i rekonstruiert, das auch von einer anderen minimalen Menge M_j rekonstruiert wird.
- Die Ergebnismenge $\mathcal{E}_B$ enthält schließlich alle Teilnehmer, die nicht zu $\mathcal{E}_E$ gehören. Für jeden Teilnehmer $P \in \mathcal{E}_B$ gilt: Jede minimale Menge, die *P* enthält, rekonstruiert ein K_i, das von keiner anderen minimalen Menge rekonstruiert wird.

In Kapitel 3.4 wird der erweiterte Test auf Konsistenz an einem (3; 6)-Threshold Scheme beispielhaft durchgeführt.

Es folgen nun vier Sätze, mit deren Hilfe gezeigt wird, dass ein Threshold Scheme in der geometrischen Realisierung durch den erweiterten Test auf Konsistenz Betrüger mit vorgebbarer Wahrscheinlichkeit identifizieren kann.

Zunächst wird die Durchschnittsmenge D näher betrachtet. Sie enthält die rekonstruierten Geheimnisse, die von mehreren minimalen Mengen rekonstruiert werden.

3.13 Satz:

Ein (t, n)-Threshold Scheme sei geometrisch in PG(t, q) wie in Definition 3.2 realisiert. Für eine zulässige Teilnehmermenge $G \in \Gamma$ werde der erweiterte Test auf Konsistenz nach Definition 3.12 durchgeführt. Wenn für die Durchschnittmenge

$$D = \{\ \}$$

gilt, dann sind weniger als $t + 1$ ehrliche Teilnehmer in G enthalten.

Beweis:
Gezeigt wird:
Wenn mindestens $t + 1$ ehrliche Teilnehmer in G enthalten sind, dann gilt $D \neq \{\ \}$.

$P_1, P_2, \ldots, P_{t+1}$ seien die ehrlichen Teilnehmer in G. Nach Definition 3.12 wird für den erweiterten Test auf Konsistenz zunächst die Minimalstruktur M ermittelt. Die Punkte der ehrlichen Teilnehmer liegen nach Definition 3.2 in dem $(t - 1)$-dimensionalen Indikatorblock in allgemeiner Lage. Daher ist jede t-elementige Untermenge von $\{P_1, P_2, \ldots, P_{t+1}\} \subseteq G$ in M enthalten.

Da die Mengen $\{P_1, P_2, \ldots, P_t\}$ und $\{P_2, P_3, \ldots, P_{t+1}\}$ denselben Schnittpunkt mit K haben, gilt nach Definition 3.12

$$D \neq \{\ \}.$$

Aus $D = \{\ \}$ folgt also, dass in der betrachteten Teilnehmermenge G weniger als $t + 1$ ehrliche Teilnehmer vorhanden sind. Das bedeutet wiederum, dass von G das tatsächliche Geheimnis K_0 nicht mehrfach rekonstruiert wird. Daher kann durch Konsistenzüberlegungen kein Betrüger mit vorgebbarer Wahrscheinlichkeit identifiziert werden. Die Aussage der Definition 3.12, nämlich

„Der erweiterte Test auf Konsistenz ist (nur dann) durchführbar, wenn $D \neq \{\ \}$“

ist also plausibel.

Der nächste Satz klärt die Frage, mit welcher Wahrscheinlichkeit in einer Teilnehmermenge mehr als t ehrliche Teilnehmer enthalten sind, wenn der Test auf Konsistenz durchführbar ist. Zu diesem Zweck ist die Frage zu klären, mit welcher Wahrschein-

lichkeit der Test für eine Teilnehmermenge mit weniger als $t + 1$ ehrlichen Teilnehmern (durch die Anwesenheit von Betrügern) durchführbar ist.

3.14 Satz:

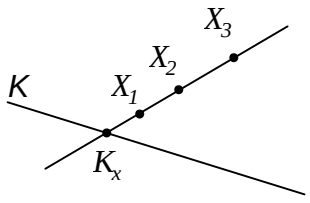
Ein (t, n)-Threshold Scheme sei geometrisch in PG(t, q) wie in Definition 3.2 realisiert. Für eine zulässige Teilnehmermenge $G \in \Gamma$ der Mächtigkeit $g > t$, die $x \leq t - 1$ Betrüger enthält, werde der erweiterte Test auf Konsistenz nach Definition 3.12 durchgeführt. Wenn für die Durchschnittmenge $D \neq \{\ \}$ gilt, dann sind mit einer Wahrscheinlichkeit von

$$p \geq 1 - \sum_{k=3}^{t+1} a_k \frac{(q^{k-1} + q^{k-2} + \ldots + q^2 - k + 2)\,(q^{k-2} + q^{k-3} + \ldots + q + 1 - k)}{(q^t + q^{t-1} + \ldots + q^2 - 1)^2}$$

$$\text{mit } a_k = \sum_{i=0}^{k-2} \binom{x}{k-i} \binom{g-x}{i}$$

mindestens $t + 1$ ehrliche Teilnehmer in G enthalten.

Beweis:



Drei Punkte liegen auf einer Geraden, es gilt $D = \{K_x\}$

Wenn k der insgesamt g Teilnehmerpunkte zusammen mit einem Punkt K_x der Geheimnisgeraden einen höchstens (k-2)-dimensionalen Raum aufspannen, dann gibt es mehrere minimale Mengen, die dasselbe Geheimnis rekonstruieren, es gilt $D \neq \{\ \}$. Beispielsweise liegen die Punkte von $t + 1$ *ehrlichen* Teilnehmern in einem (t-1)-dimensionalen Unterraum und es gilt $D \neq \{\ \}$.

Jede Konstellation von Teilgeheimnispunkten, für die $D \neq \{\ \}$ gilt, lässt sich auf k Teilnehmerpunkte, die zusammen mit K_x einen höchstens (k-2)-dimensionalen Raum aufspannen zurückführen.

Gesucht ist die Wahrscheinlichkeit dafür, dass $D \neq \{\ \}$ gilt, obwohl keine $t + 1$ ehrlichen Teilnehmer an dem erweiterten Test auf Konsistenz beteiligt sind. Das kann nur durch Anwesenheit von Betrügern passieren.

Zunächst wird die Wahrscheinlichkeit für eine solche Konstellation für $k = 3$ berechnet. Gesucht ist also die Wahrscheinlichkeit, dass 3 der insgesamt g Teilnehmerpunkte auf einer Geraden liegen, die K schneidet.

Sei a_3 die Anzahl der dreielementigen Untermengen der Teilnehmermenge, die für die obige Konstellation in Frage kommen. Das sind alle Untermengen, die ausschließlich Betrüger enthalten und alle Untermengen, die einen ehrlichen Teilnehmer und zwei Betrüger enthalten, d.h.

$$a_3 = \binom{x}{3} + \binom{x}{2}(g\text{-}x).$$

Teilmengen mit zwei ehrlichen Teilnehmern können die obige Konstellation nach Definition 3.2 nicht erfüllen, da die Punkte der Teilnehmer zusammen mit K_0 in allgemeiner Lage in dem Indikatorblock liegen und der Betrügerpunkt sich nach Definition 2.13 außerhalb des Indikatorblocks befindet.

Nun ist die Wahrscheinlichkeit dafür zu ermitteln, dass drei Punkte X_1, X_2 und X_3 aus PG(3, q) auf einer Geraden liegen, die K schneidet. Die Geheimnisgerade erzeugt mit X_1 eine Ebene. Da sich X_1, X_2 und X_3 auf einer Geraden durch K befinden sollen, muss X_2 innerhalb $\langle X_1, K\rangle$ liegen. X_2 erzeugt dann zusammen mit X_1 eine Gerade, die K schneidet. Wenn X_3 auf dieser Geraden liegt, ist $D \neq \{\ \}$ erfüllt.

Für einen Betrüger stehen zunächst alle Punkte des PG(3, q) zur Auswahl, abzüglich der Punkte der Geheimnisgeraden und seines Shadows. Das sind $q^t + q^{t-1} + \ldots + q^2 - 1$ Punkte. In der oben bezeichneten Ebene $\langle X_1, K\rangle$ gibt es $q^2 + q + 1$ Punkte, abzüglich der Punkte der Geheimnisgeraden und des ersten Teilnehmers. Auf der dann erzeugten Geraden $\langle X_1, X_2\rangle$ durch K gibt es $q + 1$ Punkte von denen der Schnittpunkt mit K und die Punkte der beiden anderen Teilnehmer abgezogen werden.

Insgesamt ergibt sich für die gesuchte Wahrscheinlichkeit:

$$p_3 \leq \frac{(q^2 - 1)(q - 2)}{(q^t + q^{t-1} + \ldots + q^2 - 1)^2}$$

Für $3 \leq k \leq g$ gilt: Die Geheimnisgerade erzeugt mit k - 2 Punkten der Teilnehmermenge einen linearen (k-1)-dimensionalen Unterraum. Liegt ein weiterer Punkt innerhalb dieses Unterraumes, so erzeugt er zusammen mit den ersten Punkten (ohne den Punkten der Geheimnisgerade) einen (k-2)-dimensionalen Unterraum, der K schneidet. Wenn der letzte der insgesamt k Punkte in diesem Unterraum liegt, ist $D \neq \{\ \}$ erfüllt.

Es gilt

$$a_k = \binom{x}{k} + \binom{x}{k\text{-}1}\binom{g\text{-}x}{1} + \ldots + \binom{x}{2}\binom{g\text{-}x}{k\text{-}2} = \sum_{i=0}^{k\text{-}2} \binom{x}{k\text{-}i}\binom{g\text{-}x}{i}$$

und

$$p_k \leq \frac{(q^{k-1} + q^{k-2} + \ldots + q^2 - k + 2)(q^{k-2} + q^{k-3} + \ldots + q + 1 - k)}{(q^t + q^{t-1} + \ldots + q^2 - 1)^2}.$$

Die Ergebnisse für $k = 3$ sind jeweils als Spezialfall enthalten.

Insgesamt ergibt sich:

$$p' \le \sum_{k=3}^{t+1} p_k a_k \quad \text{und} \quad p \ge 1 - p'$$

Anmerkung:
Für große q wird die Summe über k vom letzten Summanden bestimmt. Es gilt dann

$$\lim_{q\to\infty} p' = \frac{a_{t+1}}{q+2},$$

wobei a_k unabhängig von q ist. Die Wahrscheinlichkeit für einen Irrtum kann demnach beliebig klein vorgegeben werden.

Insgesamt ist mit den Sätzen 3.13 und 3.14 gezeigt, dass eine Teilnehmermenge $G \in \Gamma$ mit vorgebbarer Wahrscheinlichkeit mehr als $t + 1$ ehrliche Teilnehmer enthält, wenn der erweiterte Test auf Konsistenz nach Definition 3.12 durchführbar ist.

Die im Satz 3.14 angegebene Wahrscheinlichkeit wird in den folgenden Sätzen noch häufiger verwendet. Sie wird daher in der folgenden Definition festgehalten.

3.15 Definition: ERFOLGS- UND BETRUGSWAHRSCHEINLICHKEIT DES ERWEITERTEN TESTS AUF KONSISTENZ FÜR THRESHOLD SCHEMES

Ein (t, n)-Threshold Scheme sei geometrisch in PG(t, q) wie in Definition 3.2 realisiert. Für eine zulässige Teilnehmermenge $G \in \Gamma$ der Mächtigkeit $g > t$, die $x \le t - 1$ Betrüger enthält, ist die *Betrugswahrscheinlichkeit* p_B für den erweiterten Test auf Konsistenz nach Definition 3.12:

$$p_B(t) = \sum_{k=3}^{t+1} a_k \frac{(q^{k-1} + q^{k-2} + \ldots + q^2 - k + 2)\,(q^{k-2} + q^{k-3} + \ldots + q + 1 - k)}{(q^t + q^{t-1} + \ldots + q^2 - 1)^2}$$

$$\text{mit } a_k = \sum_{i=0}^{k-2} \binom{x}{k-i} \binom{g-x}{i}$$

Für die *Erfolgswahrscheinlichkeit* p_E gilt:

$$p_E(t) = 1 - p_B(t)$$

Nachdem die Bedeutung der Menge D geklärt ist, werden nun die Mengen E_E und E_B näher betrachtet.

3.16 Satz:

Ein (t, n)-Threshold Scheme sei geometrisch in PG(t, q) wie in Definition 3.2 realisiert. Für eine zulässige Teilnehmermenge $G \in \Gamma$ werde der erweiterte Test auf Konsistenz nach Definition 3.12 durchgeführt.

Wenn der Test durchführbar ist ($D \neq \{\ \}$), dann sind mit einer Wahrscheinlichkeit von $p \geq p_E$ (Definition 3.15) alle Teilnehmer, die in E_B enthalten sind, Betrüger.

Beweis:
Gezeigt wird:
Wenn der Test durchführbar ist und ein Teilnehmer ehrlich ist, dann ist er in E_E (und somit nicht in E_B) enthalten.

Nach Satz 3.14 sind in der Teilnehmermenge (mit mindestens der Wahrscheinlichkeit p_E aus Definition 3.15) $t + 1$ ehrliche Teilnehmer enthalten. Der betrachtete ehrliche Teilnehmer sei P_1, die insgesamt mindestens $t + 1$ ehrlichen seien $\{P_1, P_2, \ldots, P_{t+1}\}$.

Die ehrlichen Teilnehmer liegen in allgemeiner Lage in dem (t-1)-dimensionalen Indikatorblock, daher ist jede t-elementige Untermenge von $\{P_1, P_2, \ldots, P_{t+1}\}$ in der Minimalstruktur enthalten, die vom erweiterten Test auf Konsistenz untersucht wird. Die Anzahl der t-elementige Teilmengen von $\{P_1, P_2, \ldots, P_{t+1}\}$, die P_1 enthalten und K_0 rekonstruieren, ist t.

Nach Definition 3.12 gilt demnach $K_0 \in D$ und somit

$$P_1 \in E_E$$

Da in E_B mit der Wahrscheinlichkeit p_E kein ehrlicher Teilnehmer enthalten ist, müssen alle Teilnehmer in E_B Betrüger sein.

Anmerkung:
Die Aussage des Satzes gilt *nur* mit der Wahrscheinlichkeit $p \geq p_E$, da die Durchführbarkeit des Testes nur mit dieser Wahrscheinlichkeit sichergestellt ist (Satz 3.14).

Der nächste Satz behandelt schließlich die Bedeutung der Ergebnismenge E_E.

3.17 Satz:

Ein (t, n)-Threshold Scheme sei geometrisch in PG(t, q) wie in Definition 3.2 realisiert. Für eine zulässige Teilnehmermenge $G \in \Gamma$ werde der erweiterte Test auf Konsistenz nach Definition 3.12 durchgeführt.

Wenn der Test durchführbar ist ($D \neq \{\ \}$), dann ist mit einer Wahrscheinlichkeit von $p \geq p_E$ (Definition 3.15) ein Teilnehmer, der in E_E enthalten ist, ehrlich.

Beweis:
Nach Satz 3.16 sind alle ehrlichen Teilnehmer in E_E enthalten. Betrachtet werden muss die Wahrscheinlichkeit dafür, dass ein Betrügerpunkt in E_E enthalten ist.

Die Ergebnismenge E_E enthält alle Teilnehmer, die zu mindestens einer minimalen Menge gehören, deren rekonstruiertes Geheimnis in D enthalten ist. Gesucht ist also die Wahrscheinlichkeit dafür, dass ein Betrüger in einer solchen minimalen Menge enthalten ist.

Die Wahrscheinlichkeit dafür, dass durch das Vorhandensein von Betrügern Elemente zur Durchschnittsmenge D hinzugefügt werden, wurde im Beweis zu Satz 3.14 als $p \geq p_E$ ermittelt. Genau mit dieser Wahrscheinlichkeit sind auch Betrüger in E_E enthalten.

Mit den Aussagen der vorangegangenen vier Sätze kann gezeigt werden, dass sich der erweiterte Test auf Konsistenz eignet, einen Betrüger mit vorgebbarer Wahrscheinlichkeit zu identifizieren.

3.18 Satz:

Ein (t, n)-Threshold Scheme sei geometrisch in PG(t, q) wie in Definition 3.2 realisiert. Wenn die Eingaben der Teilnehmer vor der Geheimnisrekonstruktion durch den erweiterten Test auf Konsistenz nach Definition 3.12 überprüft werden, dann ist das Threshold Scheme nach Definition 2.15 *stark robust*.

Betrüger werden mit einer Wahrscheinlichkeit von $p \geq p_E$ (Definition 3.15) identifiziert und sind in der Ergebnismenge E_B enthalten.

Beweis:
Die Aussagen des Satzes folgen sofort aus den Sätzen 3.13, 3.14, 3.16 und 3.17.

Ein geometrisch realisiertes Threshold Scheme, dessen Zugriffskontrollinstanz den erweiterten Test auf Konsistenz durchführt, ist demnach stark robust. Die Teilnehmer in den Ergebnismengen E_B bzw. E_E sind mit einer Wahrscheinlichkeit von $p \geq p_E$ Betrüger bzw. ehrliche Teilnehmer.

3.4 Beispiel

Abschließend zu den Betrachtungen zu den Threshold Schemes wird in diesem Abschnitt ein Beispiel für die Durchführung des erweiterten Testes auf Konsistenz gegeben.

Ein (3; 6)-Threshold Scheme sei geometrisch realisiert. Die Teilnehmer P_1, P_2, P_3 und P_4 seien ehrlich, die Teilnehmer P_5 und P_6 seien Betrüger. Die Lage ihrer Teilgeheimnisse ist in Abbildung 15 dargestellt.

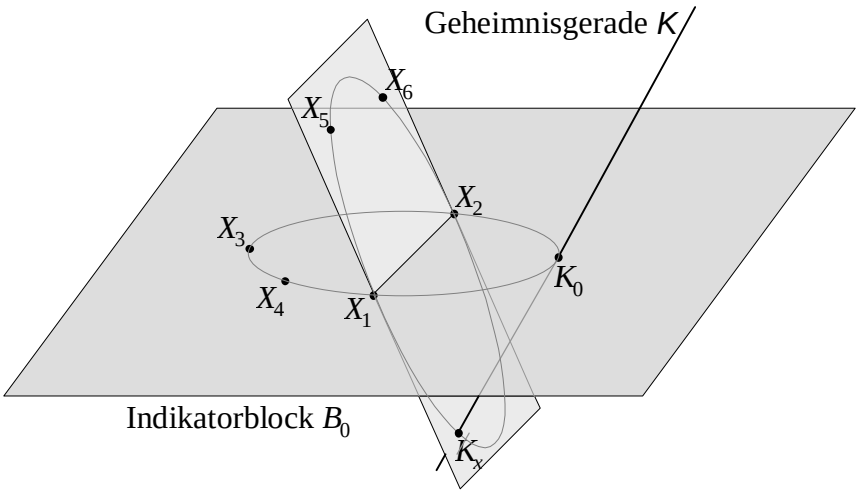


Abbildung 15: Ein (3; 6)-Threshold Scheme mit zwei Betrügern

In den nächsten Abschnitten werden verschiedene Teilnehmermengen zusammengestellt und jeweils der erweiterte Test auf lineare Konsistenz nach Definition 3.12 durchgeführt. Die Bedeutung der einzelnen Ergebnismengen wird erklärt.

3.4.1 Test nicht durchführbar

In der Teilnehmermenge seien drei ehrliche Teilnehmer und ein Betrüger enthalten:

$$G = \{P_1, P_2, P_3, P_5\}$$

Für den erweiterten Test auf Konsistenz werden zunächst alle minimalen Mengen benötigt. Diese sind:

$$M_1 = \{P_1, P_2, P_3\}$$
$$M_2 = \{P_2, P_3, P_5\}$$
$$M_3 = \{P_3, P_5, P_1\}$$
$$M_4 = \{P_5, P_1, P_2\}$$

Nun sind nach Definition 3.12 die K_i zu berechnen. Jede dieser minimalen Mengen erzeugt eine Ebene, die genau einen Schnittpunkt mit der Geheimnisgeraden hat. Die Schnittpunkte sind nach Abbildung 15 unterschiedlich. Es gilt

$$K_1 \neq K_2 \neq K_3 \neq K_4.$$

Demzufolge gilt $D = \{\ \}$ und der Test ist nicht durchführbar.

Anmerkung:
An dieser Teilnehmerkonstellation lässt sich ein Nachteil aufzeigen, den der Test auf Konsistenz durch minimale Mengen (nach Definition 3.9) gegenüber dem einfachen Test auf Konsistenz (nach Definition 3.4) hat.
Die Zugriffskontrollinstanz würde durch den Test auf Konsistenz nach Definition 3.4 nämlich bei der obigen Konstellation wenigstens den Betrug bemerken. Sie würde die Schwelle t kennen und feststellen, dass $t + 1$ Teilnehmer in G enthalten sind und somit die K_i nur durch Anwesenheit von Betrügern unterschiedlich sein können. Für den Test auf Konsistenz durch minimale Mengen hingegen werden $t + 1$ *ehrliche* Teilnehmer gefordert, damit er überhaupt durchführbar ist.
Dieser Nachteil wird jedoch dadurch relativiert, dass die Teilnehmer durch den einfachen Test auf Konsistenz zwar wissen, dass ein Betrug stattgefunden hat, jedoch den Betrüger und vor allem das wahre K_0 nicht kennen. Nach dem Feststellen eines Betruges müsste beim Test auf Konsistenz zur Beantwortung dieser Fragen ebenfalls ein weiterer ehrlicher Teilnehmer gesucht werden.

3.4.2 Test wird bestanden

Seien nun in der Teilnehmermenge die vier ehrlichen Teilnehmer enthalten:

$$G = \{P_1, P_2, P_3, P_4\}$$

Erneut werden zunächst alle minimalen Mengen benötigt. Diese sind:

$$M_1 = \{P_1, P_2, P_3\}$$

$$M_2 = \{P_2, P_3, P_4\}$$

$$M_3 = \{P_3, P_4, P_1\}$$

$$M_4 = \{P_4, P_1, P_2\}$$

Nach Definition 3.12 werden die K_i berechnet. Da die Punkte der Teilnehmer in der Indikatorebene in allgemeiner Lage mit K_0 liegen, schneidet das Erzeugnis jeder minimalen Menge die Geheimnisgerade in demselben Punkt. Es gilt

$$K_1 = K_2 = K_3 = K_4\ (= K_0).$$

Demzufolge gilt $D = \{K_0\}$ und der Test ist durchführbar. Die Menge G besteht den Test, da alle K_i aus einem Element bestehen und alle diese Elemente gleich sind.

Da alle minimalen Mengen dasselbe Geheimnis rekonstruieren gilt

$$E_E = G$$

und

$$E_B = \{\ \},$$

d.h. alle Teilnehmer werden als ehrlich erkannt.

3.4.3 Test wird nicht bestanden

Seien in einem weiteren Beispiel in der Teilnehmermenge die vier ehrlichen Teilnehmer und ein Betrüger enthalten:

$$G = \{P_1, P_2, P_3, P_4, P_5\}$$

Zunächst werden alle minimalen Mengen benötigt. Diese sind:

$$M_1 = \{P_1, P_2, P_3\},$$

$$M_2 = \{P_2, P_3, P_4\},$$

$$M_3 = \{P_3, P_4, P_1\},$$

$$M_4 = \{P_4, P_1, P_2\},$$

sowie sechs weitere minimale Mengen $M_5, M_6, \ldots, M_{10}$ mit dem Betrüger P_5 und je zwei ehrlichen Teilnehmern.

Nach Definition 3.12 werden die K_i berechnet. Es gilt

$$K_1 = K_2 = K_3 = K_4 \ (= K_0) \text{ und}$$

$$K_5 \neq K_6 \neq K_7 \neq K_8 \neq K_9 \neq K_{10} \ (\neq K_0).$$

Demzufolge gilt $D = \{K_0\}$ und der Test ist durchführbar. Die Menge G besteht den Test nicht, da alle K_i zwar aus einem Element bestehen, diese aber nicht alle gleich sind.

Da nur die minimalen Mengen M_1 bis M_4 dasselbe Geheimnis rekonstruieren gilt

$$E_E = \{P_1, P_2, P_3, P_4\}$$

und

$$E_B = \{P_5\},$$

d.h. der Betrüger P_5 wird erkannt.

3.4.4 Test rekonstruiert ein falsches Ergebnis

In dem letzten Beispiel seien in der Teilnehmermenge drei ehrliche Teilnehmer und die beiden Betrüger enthalten:

$$G = \{P_1, P_2, P_3, P_5, P_6\}$$

Die minimalen Mengen sind:

$$M_1 = \{P_1, P_2, P_5\},$$

$$M_2 = \{P_2, P_5, P_6\},$$

$$M_3 = \{P_5, P_6, P_1\},$$

$$M_4 = \{P_6, P_1, P_2\},$$

sowie sechs weitere minimale Mengen M_5, M_6, …, M_{10}, die den ehrlichen Teilnehmer P_3 sowie zwei weitere Teilnehmer enthalten.

Nach Definition 3.12 werden die K_i berechnet. Wie in Abbildung 15 dargestellt, liegen die Punkte der Teilnehmer P_1, P_2, P_5 und P_6 in einer Ebene. Alle minimalen Mengen, die drei dieser Teilnehmer enthalten, rekonstruieren dasselbe Geheimnis K_x. Es gilt

$$K_1 = K_2 = K_3 = K_4 \ (= K_x) \text{ und}$$

$$K_5 \neq K_6 \neq K_7 \neq K_8 \neq K_9 \neq K_{10} \ (\neq K_x).$$

Demzufolge gilt $D = \{K_x\}$ und der Test ist durchführbar (obwohl keine $t + 1$ ehrlichen Teilnehmer an der Rekonstruktion teilnehmen). Die Menge G besteht den Test nicht, da alle K_i zwar aus einem Element bestehen, diese aber nicht alle gleich sind.

Da die minimalen Mengen M_1 bis M_4 dasselbe Geheimnis rekonstruieren gilt

$$E_E = \{P_1, P_2, P_5, P_6\}$$

und

$$E_B = \{P_3\},$$

d.h. die Betrüger P_5 und P_6 bleiben als Betrüger unerkannt und der ehrliche Teilnehmer P_3 wird als Betrüger identifiziert.

Diese Situation kann mit einer Wahrscheinlichkeit von $p \geq p_E$ (Definition 3.15) ausgeschlossen werden.

4. Compartment Schemes

Compartment Schemes wurden mit Definition 2.9 eingeführt. Es handelt sich um Secret Sharing Schemes, bei denen mehrere Klassen von Teilnehmern der Rekonstruktion zustimmen müssen. Für die Zustimmung einer Klasse ist eine Mindestanzahl von Teilnehmern erforderlich. Die Klassen werden Compartments ($C_1, \ldots, C_r$) genannt, die Schwellen innerhalb der einzelnen Compartments sind $t_1, \ldots, t_r$. Die Anzahl der Compartments, die für eine erfolgreiche Rekonstruktion mindestens teilnehmen müssen, ist t.

Die einfachste Realisierungsmöglichkeit für Compartment Schemes ist eine Kombination von Threshold Schemes. Für jedes Compartment wird ein Threshold Scheme konstruiert, die verschlüsselten Geheimnisse der einzelnen Threshold Schemes sind die Teilgeheimnisse eines übergeordneten Threshold Schemes. Dieses rekonstruiert das eigentliche Geheimnis, sofern genügend Compartments zustimmen.

Die genannte Lösung ist jedoch nur für gewisse Compartment Schemes sinnvoll. Sie kann dann angewendet werden, wenn die Zugriffskontrollinstanz in der Lage ist, die Teilnehmer den Compartments zuzuordnen. Dies wäre beispielsweise der Fall, wenn die Teilnehmer ihre Teilgeheimnisse an verschiedenen Orten entsprechend ihrer Zugehörigkeit zu den Compartments eingeben. Wenn jedoch für ein Secret Sharing Scheme gefordert wird, dass die Teilnehmer ungeordnet ihre Teilgeheimnisse an eine Zugriffskontrollinstanz weitergeben können, dann kann diese nicht entscheiden, welchem der r Threshold Schemes ein eingegebener Shadow zugeordnet werden soll. Eine Rekonstruktion ist dann nicht möglich.

Die im folgenden Abschnitt definierte geometrische Realisierung für Compartment Schemes gewährleistet, dass eine Kontrollinstanz den Zugriff überprüfen kann, ohne die Zugehörigkeit der Teilnehmer zu den Compartments zu kennen.

4.1 Geometrische Compartment Schemes

Simmons hat zwei Verfahren zur Konstruktion von Compartment Schemes angegeben [Sim89]. Diese Verfahren wurden von Kersten erweitert und zu einer allgemeingültigen Konstruktion zusammengefasst [Ker92]. Im folgenden wird dieses zusammengefasste Verfahren beschrieben.

In Kapitel 3.1 wurden die geometrischen Secret Sharing Schemes im allgemeinen eingeführt und anschließend die Threshold Schemes im speziellen definiert. Hier werden diese allgemeinen Bezeichnungen für Secret Sharing Schemes für die Compartment Schemes aus Definition 2.9 spezifiziert.

4.1 Definition: GEOMETRISCHE COMPARTMENT SCHEMES

Ein *geometrisches (t; t_1, …, t_r)-Compartment Scheme* wird als geometrisches Secret Sharing Scheme wie in Definition 3.1 realisiert [Ker92].

Für die Dimension *d* des projektiven Raumes PG(*d*, *q*) gilt:

$$d := (t_1\text{-}1) + (t_2\text{-}1) + \ldots + (t_r\text{-}1) + (t\text{-}1) + s$$

Ferner sind gegeben:

- Ein Unterraum B_0^* mit
  $d^* := \dim B_0^* = (t_1\text{-}1) + (t_2\text{-}1) + \ldots + (t_r\text{-}1) + (t\text{-}1)$ und
  $B_0^* \cap K = K_0$.
- Ein (*t*-1)-dimensionaler linearer Unterraum B_0 von B_0^* mit
  $B_0 \cap K = K_0$
- *r* Punkte $p_1, p_2, \ldots, p_r$ von B_0, die zusammen mit K_0 in allgemeiner Lage sind.
- *r* Unterräume $B_1, B_2, \ldots, B_r$ in B_0^* mit den folgenden Eigenschaften:
  1. Die Unterräume $B_1, B_2, \ldots, B_r$ sind paarweise disjunkt und treffen den Geheimnisraum *K* nicht.
  2. $\dim B_i = t_i - 1 \quad (i = 1, 2, \ldots, r)$
  3. $B_i \cap B_0 = B_i \cap \langle B_0; K\rangle = p_i \qquad (i = 1, 2, \ldots, r)$
  4. Für $i = 1, 2, \ldots, r$ gilt: $B_i \notin \langle \{B_1, B_2, \ldots, B_r\} \backslash \{B_i\}\rangle$
  5. Je *t* der Unterräume $B_1, B_2, \ldots, B_r$ sind unabhängig, d.h. für alle $j \in \{1, 2, \ldots, t\}$ gilt: $\langle \{B_{i_1}, B_{i_2}, \ldots, B_{i_t}\} \backslash \{B_{i_j}\}\rangle \cap \{B_{i_j}\} = \{\ \}$.
- In den linearen Unterräumen B_i ist jeweils eine Menge E_i von Punkten gegeben, für die gilt:
  6. $|E_i| = |C_i| =: n_i \quad (i = 1, 2, \ldots, r)$
  7. $p_i \notin E_i \quad (i = 1, 2, \ldots, r)$
  8. Je t_i Punkte aus $E_i \cup \{p_i\}$ erzeugen den Unterraum B_i.$(i = 1, 2, \ldots, r)$

Jeder Teilnehmer aus dem Compartment C_i erhält einen Punkt aus E_i als Teilgeheimnis. Die Teilgeheimnisse verschiedener Teilnehmer sind unterschiedlich.

Anmerkungen:

- Jedes geometrische Compartment Scheme ist perfekt [Ker92].
- Die Unterräume $B_1, B_2, \ldots, B_r$ werden wie folgt konstruiert [Ker92]:
  - B_1 wird durch p_1 gewählt mit: $B_1 \cap \langle B_0; K\rangle = p_1$
  - Für $i = 2, \ldots, t$ wird B_i durch p_i gewählt mit: B_i ist disjunkt zu $\langle B_1; \ldots; B_{i-1}\rangle$ und $\langle B_1; \ldots; B_i\rangle \cap \langle B_0; K\rangle = \langle p_1; \ldots; p_i\rangle$
  - Für $i = t + 1, \ldots, r$ wird B_i durch p_i gewählt mit: $\langle B_1; \ldots; B_{i-1}\rangle \cap \langle B_i\rangle = p_i$ und jede *t*-elementige Teilmenge von $\{B_1, \ldots, B_i\}$ ist unabhängig.

Nach obiger Definition wird die Zugehörigkeit von Teilgeheimnissen zu Compartments durch die Lage der Teilgeheimnisse in den Unterräumen B_1, B_2 , …, B_r bestimmt. Ähnlich wie bei den Threshold Schemes spannen die Teilnehmer des Compartments C_i einen t_i-dimensionalen Unterraum auf, in dem n_i Punkte (gemeinsam mit p_i) in allgemeiner Lage sind.

Durch die Bedingungen 4. und 5. der Definition wird gewährleistet, dass nichtzulässige Teilnehmerkonfigurationen K_0 nicht rekonstruieren können. Wenn Bedingung 4. erfüllt ist, dann kann kein Compartment durch eine Kombination von (bis zu r-1) anderen Compartments ersetzt werden. Durch Bedingung 5. wird sichergestellt, dass durch eine Kombination von (bis zu t-1) Compartments kein Teilnehmer eines anderen Compartments ersetzt werden kann [Ker92]. Die Zugriffskontrollinstanz braucht daher für die Rekonstruktion keine weiteren Informationen als die Teilnehmerpunkte.

Die folgende Abbildung zeigt ein geometrisch realisiertes (3; 3, 2, 2, 2)-Compartment Scheme. Es wird in PG(8, q) realisiert.

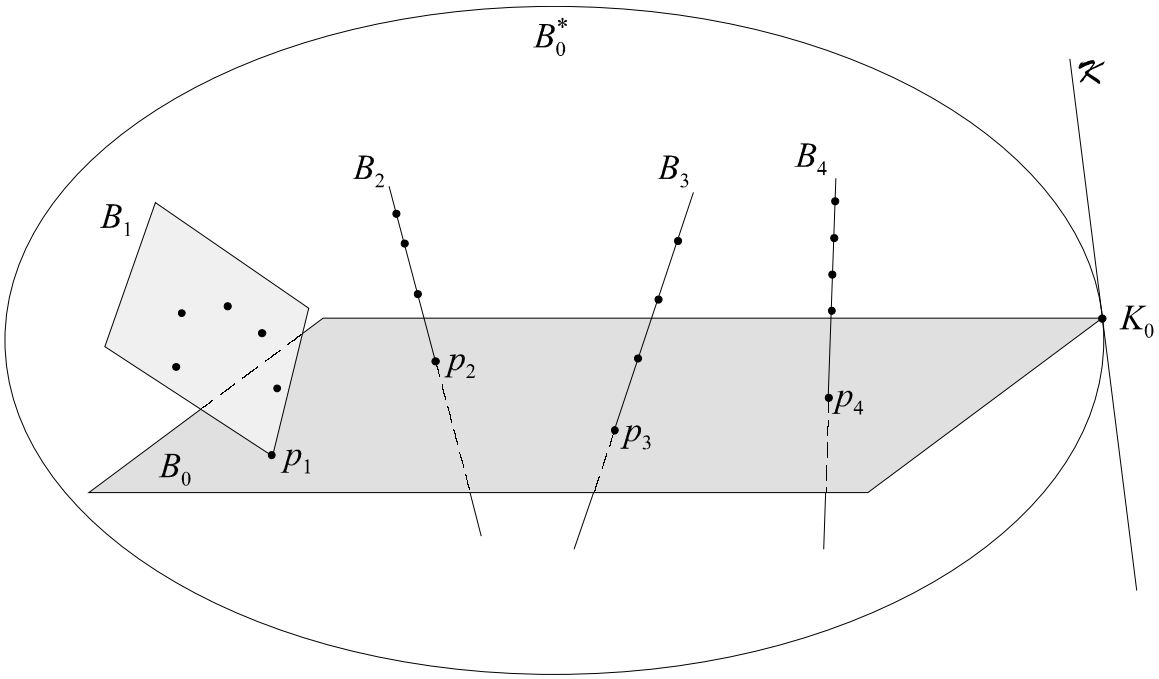


Abbildung 16: Ein geometrisches Compartment Scheme

Die Blöcke B_1, B_2, B_3, B_4 sind unabhängig voneinander.

4.2 Erkennen eines Betruges

4.2.1 Test auf Konsistenz

Der Test auf Konsistenz für Threshold Schemes wurde in Kapitel 3.2 vorgestellt. Ein ähnlicher Test für Compartment Schemes wird im folgenden dargestellt [Neh93].

Zunächst wird die Kontrollstruktur für Compartment Schemes definiert. Mit dieser Kontrollstruktur wird später der Test auf Konsistenz durchgeführt.

4.2 Definition: KONTROLLSTRUKTUR FÜR COMPARTMENT SCHEMES

Sei $P = \{P_1, P_2, \ldots, P_n\}$ die Teilnehmermenge eines Secret Sharing Schemes und seien $C_1, C_2, \ldots, C_r$ Compartments wie in Definition 2.9.

Seien $t_1, t_2, \ldots, t_r$ natürliche Zahlen mit $t_i \le |C_i|$ für $i = 1, 2, \ldots, r$ und t eine natürliche Zahl mit $t \le r$. Eine Menge $\Phi \subseteq \mathbf{P}(P)$ mit

$$\Phi := \left\{ F \in \mathbf{P}(P) \;\middle|\; \text{es gibt } F_{i_1}, F_{i_2}, \ldots, F_{i_k} \in \{C_1, C_2, \ldots, C_r\} \right.$$
$$\left. \text{mit } t+1 \le k \le r \text{ und } \left|F_{i_j} \cap F\right| \ge t_{i_j} + 1 \text{ für } j = 1, 2, \ldots, k \right\}$$

heißt (t; $t_1, t_2, \ldots, t_r$)-*Compartment-Scheme-Kontrollstruktur*.

Die in der Kontrollstruktur enthaltenen Teilnehmermengen F heißen *Kontrollmengen*.

Gemäß obiger Definition ist in der Kontrollstruktur für den Test auf Konsistenz nach [Neh93]

- in jedem Compartment mindestens ein zusätzlicher Teilnehmer und
- darüber hinaus mindestens ein Compartment mehr

enthalten als nach Definition 2.9 zur Rekonstruktion des Geheimnisses erforderlich wäre.

Anmerkung:
In Kapitel 4.2.2 werden grundlegende Überlegungen zur minimalen Mächtigkeit, die eine Kontrollstruktur für einen Konsistenztest besitzen muss, vorgestellt.

Bevor der Test auf Konsistenz für Compartment Schemes definiert wird, werden ergänzend zu den Definitionen 2.1 und 2.2 noch eine weitere Basismenge von Blöcken und zwei zusätzliche Basisabbildungen eingeführt.

4.3 Definition: ERWEITERTE BASISMENGEN UND BASISABBILDUNGEN

Seien

A	eine Menge von *Präblöcken*,
δ: $\mathbf{P}(X) \rightarrow \mathbf{P}(A)$	eine Abbildung von Mengen von Teilgeheimnissen auf Mengen von Präblöcken sowie
$\lambda \subseteq \mathbf{P}(A) \times B$	eine Relation zwischen Mengen von Präblöcken und Blöcken.

Die folgende Abbildung zeigt den Zusammenhang der in den Definitionen 2.1, 2.2 und 4.3 eingeführten Basismengen und -abbildungen.

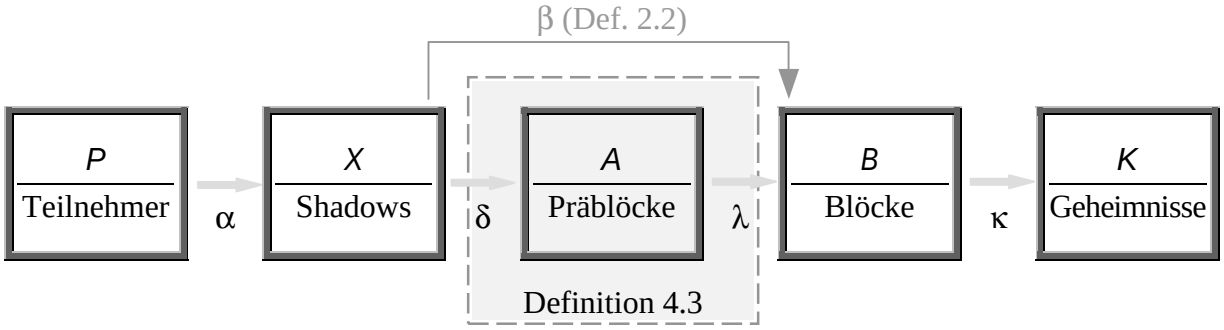


Abbildung 17: Erweiterte Basismengen und -abbildungen

Die neuen Basismengen und -abbildungen werden durch die folgende Definition für die geometrische Realisierung von Compartment Schemes konkretisiert.

4.4 Definition: ERWEITERTE GEOMETRISCHE COMPARTMENT SCHEMES

Sei V := $\langle K, B_0 \rangle$.

a) Die Menge der Präblöcke $A = A_1 \cup A_2 \cup \ldots \cup A_r$ ist definiert als die Menge der linearen Unterräume von V.

b) Die Abbildung δ: $\mathbf{P}(X) \rightarrow \mathbf{P}(A)$ ist für $Y \subseteq X$ und $A \subseteq A$ definiert als

$$\delta(Y) := \{\langle Y \cap C_1 \rangle \cap V, \langle Y \cap C_2 \rangle \cap V, \ldots, \langle Y \cap C_r \rangle \cap V\}$$
$$=: \{A_1, A_2, \ldots, A_r\} = A,$$

wobei r die Anzahl der Compartments ist.

c) Die Relation $\lambda \subseteq \mathbf{P}(A) \times B$ ist für alle $A \subseteq A$ und $B \in B$ definiert als:

$$(A, B) \in \lambda \quad \Leftrightarrow \quad \langle A \rangle \leq B$$

Mit diesen Definitionen wird nun der Test auf Konsistenz für Compartment Schemes eingeführt:

4.5 Definition: TEST AUF KONSISTENZ (COMPARTMENT SCHEMES)

Sei $F \in \Phi$ mit $F = F_1 \cup F_2 \cup \ldots \cup F_m$ und $F_i := F \cap C_i$.

Der Test auf Konsistenz für Compartment Schemes besteht aus zwei Teilen:

1.) Sei $c_i := |F_i|$, also gleich der Anzahl der Teilnehmer aus F, die in C_i enthalten sind und

$$f_i := \binom{c_i}{t_i}$$

die Anzahl der t_i-elementigen Teilmengen von $F_i = F \cap C_i$.

Aus den t_i-elementigen Teilmengen F_i^j ($j = 1, 2, \ldots, f_i$) werden die Mengen $A_i{}^j$ wie folgt gebildet:

$$A_i{}^1 := \delta(\alpha_K(F_i{}^1))$$
$$\vdots$$
$$A_i{}^{f_i} := \delta(\alpha_K(F_i{}^{f_i}))$$

Der erste Teil des Tests ist bestanden, wenn (für $j = 1, 2, \ldots, f_i$ und jedes feste i) die Mengen $A_i{}^j$ aus einem Element bestehen und diese Elemente gleich sind.

2.) Sei

$$N = \{ A_1{}^1, A_2{}^1, \ldots, A_m{}^1 \}.$$

Ferner sei

$$f := \binom{m}{t}.$$

Aus der Menge N werden alle t-elementigen Teilmengen N_k gebildet ($k = 1, 2, \ldots, f$). Für jedes $N_k \subseteq N$ werden die Mengen B_k und K_k wie folgt gebildet:

$$B_1 := \left\{ B \in B \middle| (N_1, B) \in \lambda \right\}$$
$$K_1 := \left\{ K \in K \middle| \kappa(B) = K \text{ für alle } B \in B_1 \right\}$$
$$\vdots$$
$$B_f := \left\{ B \in B \middle| (N_f, B) \in \lambda \right\}$$
$$K_f := \left\{ K \in K \middle| \kappa(B) = K \text{ für alle } B \in B_f \right\}$$

Die Menge F besteht den Test, wenn alle Mengen K_k aus einem Element bestehen und diese Elemente gleich sind.

Der erste Teil des beschriebenen Tests auf Konsistenz kontrolliert die Rekonstruktion innerhalb der einzelnen Compartments. Die Zugriffskontrollinstanz überprüft, ob alle t_i-elementigen Teilmengen des Compartments C_i denselben Präblock rekonstruieren.

Der zweite Teil des Tests überprüft die Konsistenz im Zusammenwirken der Compartments. Dazu wird aus den Mengen A_i^1 die Menge N gebildet. Die Mengen A_i^1 enthalten die rekonstruierten Schnittmengen für ein Compartment C_i. Analog zum Test auf Konsistenz für Threshold Schemes (Definition 3.4) werden für jede t-elementige Teilmenge N_k von N die Indikatorblöcke und die Schnittpunkte mit der Geheimnisgeraden gebildet. Wenn die Ergebnisse für alle N_k gleich sind, ist der Test bestanden.

Der Ablauf des Tests ist in der folgenden Abbildung verdeutlicht.

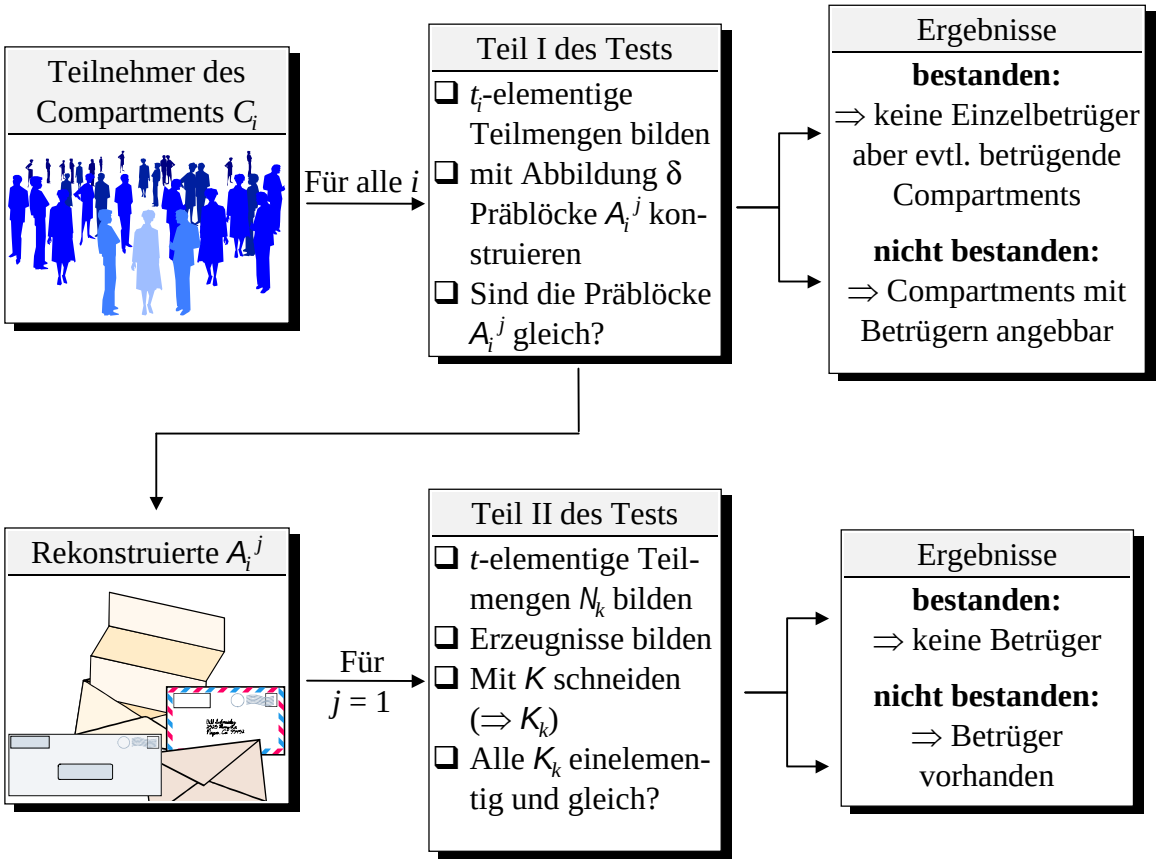


Abbildung 18: Verlauf des Tests auf Konsistenz für Compartment Scheme

Folgende Informationen braucht der dargestellte Test auf Konsistenz:

- Die Teilgeheimnisse der Teilnehmer,
- für jeden Teilnehmer das Compartment, zu dem er gehört, und
- die Schwellen (innerhalb der Compartments und für die insgesamt benötigten Compartments).

Der Test ist daher in Bezug auf die in Kapitel 1.7 formulierte Zielsetzung, dem Secret Sharing Scheme solle über die Shadows der Teilnehmer hinaus keine weitere Information zur Verfügung gestellt werden, unbefriedigend.

Ferner verliert die Realisierung der Compartment Schemes durch den Test auf Konsistenz an Vielseitigkeit. Der wesentliche Vorteil der in Definition 4.1 eingeführten Realisierung von Compartment Schemes besteht darin, dass die Kontrollinstanz für die Rekonstruktion dieselben Schritte ausführen muss, wie bei den Threshold Schemes. Diese Schritte sind

- das Erzeugnis der Punkte bilden und
- dieses Erzeugnis mit K schneiden.

Der Test auf Konsistenz setzt die Realisierung des Compartment Schemes mit Hilfe von Präblöcken gemäß Definition 4.4 voraus und damit geht dieser Vorteil verloren. Definition 4.4 entspricht bei näherer Betrachtung der zu Beginn des Kapitels 4 diskutierten und verworfenen Lösung kombinierter Threshold Schemes zur Realisierung eines Compartment Schemes.

Daher wird der Test auf Konsistenz nach Definition 4.5 nicht weiter untersucht. In Abschnitt 4.2.3 wird ein erweiterter Test auf Konsistenz vorgestellt, der ohne die oben genannten Zusatzinformationen auskommt. Vorher werden jedoch allgemeine Überlegungen zur Mächtigkeit der Kontrollstruktur angestellt.

4.2.2 Abschätzung der Mächtigkeit der Kontrollstruktur

In Definition 4.2 wurde die Kontrollstruktur für Compartment Schemes vorgestellt. In dieser Kontrollstruktur wird für jedes Compartment mindestens ein Teilnehmer mehr und zusätzlich mindestens ein Compartment mehr, als zur Rekonstruktion benötigt, gefordert. In diesem Abschnitt wird geklärt, wie viele Teilgeheimnisse ein Konsistenztest mindestens benötigt, um die Frage, ob ein Betrug stattgefunden hat, beantworten zu können.

Der folgende Satz gibt diese Untergrenze für die Mächtigkeit der Kontrollstruktur an. Dabei wird davon ausgegangen, dass durch einen Test jedes Teilgeheimnis auf Konsistenz geprüft werden soll. Die Betrachtungen sind von der konkreten Realisierung des Compartment Schemes unabhängig.

4.6 Satz:

Sei F eine zulässige Teilnehmermenge eines Compartment Schemes (Definition 2.9). Durch einen Test auf Konsistenz (Definition 2.17) kann nur dann die Konsistenz des rekonstruierten Geheimnisses für F geprüft werden, wenn

$$C_{i_1}, C_{i_2}, \ldots, C_{i_t} \in \{C_1, C_2, \ldots, C_r\} \text{ mit } |C_{i_j} \cap F| \geq t_{i_j} + 1 \text{ für } j = 1, 2, \ldots, t$$

oder

$$C_{i_1}, C_{i_2}, \ldots, C_{i_{t+1}} \in \{C_1, C_2, \ldots, C_r\} \text{ mit } |C_{i_j} \cap F| \geq t_{i_j} \text{ für } j = 1, 2, \ldots, t+1$$

existieren.

Beweis:
Das Rekonstruktionsergebnis von F soll bezüglich jedes eingegebenen Teilgeheimnisses auf Konsistenz geprüft werden. Das ist nur möglich, wenn für jeden Teilnehmer mindestens eine Teilmenge T von F, gebildet werden kann,

- in der er *nicht* enthalten ist und
- die genügend Teilnehmer für die Rekonstruktion beinhaltet.

Die Kontrollmenge F kann mit dieser Teilmenge T dahingehend auf Konsistenz geprüft werden, ob durch die Anwesenheit des Teilnehmers in F das Rekonstruktionsergebnis verändert wird.

Zu zeigen ist: Wenn keine der beiden Voraussetzungen des Satzes erfüllt ist, dann gibt es Teilnehmer, für die kein Konsistenztest durchgeführt werden kann.

Sei

- $|C_k \cap G| \geq t_k$ für $k = i_1, i_2, \ldots, i_t$ und
- $|C_k \cap G| < t_k$ für $k \neq i_1, i_2, \ldots, i_t$ und
- $|C_k \cap G| < t_k + 1$ für mindestens ein $k \in \{i_1, i_2, \ldots, i_t\}$.

Sei C_j das Compartment, welches (nach Definition 2.10) minimal in F ist. Dann wird die Teilnehmermenge F durch Entfernen eines Teilnehmers P aus C_j unzulässig, da die Bedingungen für Zulässigkeit nach Definition 2.9 von $F \setminus P$ nicht mehr erfüllt werden. Daher kann die Konsistenz bezüglich der Teilnehmer aus C_j nicht geprüft werden.

Satz 4.6 sagt, dass ein Konsistenztest (wenn überhaupt) nur dann durchgeführt werden kann, wenn

- in jedem an der Rekonstruktion beteiligten Compartment mindestens ein Teilnehmer zu viel enthalten ist (dann bleibt die Teilnehmermenge durch Weglassen eines Teilnehmers zulässig, weil sein Compartment noch mit ausreichend vielen Teilnehmern vertreten ist), oder
- mindestens ein Compartment mehr, als benötigt, an der Rekonstruktion teilnimmt (dann bleibt die Teilnehmermenge durch Weglassen eines Teilnehmers zulässig, weil noch genügend Compartments an der Rekonstruktion teilnehmen).

4.2.3 Compartments ermitteln

In diesem Abschnitt wird gezeigt, wie die Zugriffskontrollinstanz unter gewissen Voraussetzungen in der Lage ist, nur aus den Informationen der eingegebenen Teilgeheimnisse die Compartments zu identifizieren.

Anhand des folgenden Beispiels wird zunächst die Idee vorgestellt, auf der die Ermittlung der Compartments beruht.

Beispiel:
Gegeben sei ein (3; 2, 2, 2, 2)-Compartment Scheme wie in der folgenden Abbildung dargestellt.

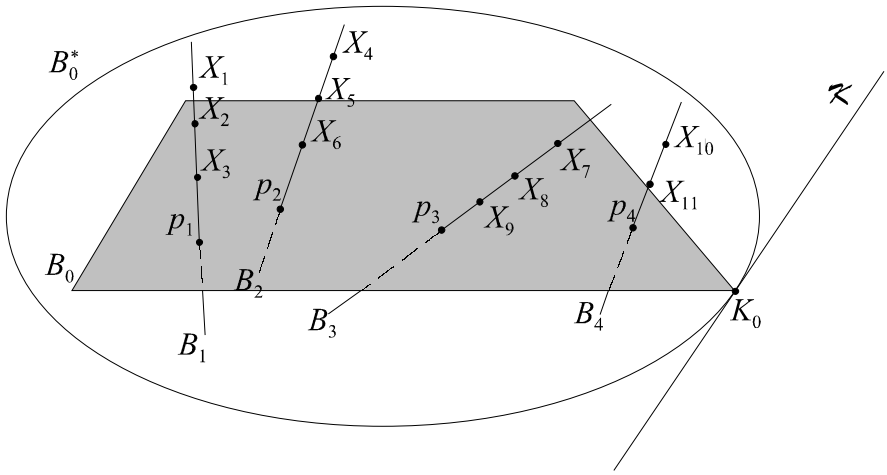


Abbildung 19: Ein (3; 2, 2, 2, 2)-Compartment Scheme

An der Rekonstruktion soll die Menge

$$G = P \setminus \{P_9, P_{11}\} = \{P_1, P_2, \ldots, P_8, P_{10}\}$$

teilnehmen. Das bedeutet, dass in den Compartments C_1 und C_2 je ein Teilnehmer mehr, als für die Rekonstruktion erforderlich, vorhanden ist. In C_3 ist genau die notwendige Anzahl Teilnehmer verfügbar. Der Teilnehmer P_{10} aus Compartment C_4 trägt nicht zur Rekonstruktion bei.

Es gibt nach Definition 2.11 neun minimale Mengen. Diese sind in der folgenden Tabelle eingetragen. In den Spalten- bzw. Zeilenköpfen sind jeweils diejenigen Teilnehmer eingetragen, die in *jeder* minimalen Menge der Spalte bzw. Zeile vorkommen.

	P_4,P_5,P_7,P_8	P_4,P_6,P_7,P_8	P_5,P_6,P_7,P_8
P_1,P_2,P_7,P_8	$M_1 = \{P_1,P_2,P_4,P_5,P_7,P_8\}$	$M_4 = \{P_1,P_2,P_4,P_6,P_7,P_8\}$	$M_7 = \{P_1,P_2,P_5,P_6,P_7,P_8\}$
P_1,P_3,P_7,P_8	$M_2 = \{P_1,P_3,P_4,P_5,P_7,P_8\}$	$M_5 = \{P_1,P_3,P_4,P_6,P_7,P_8\}$	$M_8 = \{P_1,P_3,P_5,P_6,P_7,P_8\}$
P_2,P_3,P_7,P_8	$M_3 = \{P_2,P_3,P_4,P_5,P_7,P_8\}$	$M_6 = \{P_2,P_3,P_4,P_6,P_7,P_8\}$	$M_9 = \{P_2,P_3,P_5,P_6,P_7,P_8\}$

Auffällig ist, dass in allen minimalen Mengen die Teilnehmer P_7 und P_8 vorkommen. Das ist verständlich, wenn beachtet wird, dass aus dem Compartment C_3 mit P_7 und P_8 genau so viele Teilnehmer stammen, wie zur Rekonstruktion erforderlich sind und das Compartment C_3 insgesamt für die Rekonstruktion gebraucht wird. Die Teilnehmer des minimal vertretenen Compartments C_3 lassen sich also in diesem Beispiel einfach entdecken.

Der Teilnehmer P_{10} kommt in keiner der minimalen Mengen vor. Er trägt nicht zur Rekonstruktion bei.

Etwas komplexer sind die Zusammenhänge für die Teilnehmer aus den Compartments C_1 und C_2. Bei Betrachtung der ersten Tabellenzeile wird deutlich, dass dort genau die minimalen Mengen eingetragen sind, die den Teilnehmer P_3 *nicht* enthalten. In allen diesen minimalen Mengen kommen die Teilnehmer P_1 und P_2 vor, wie auch aus dem Zeilenkopf der ersten Zeile zu entnehmen ist.

Auch dieser Sachverhalt ist nachvollziehbar. In der ersten Zeile der Tabelle stehen genau die minimalen Mengen der Teilnehmermenge $G \setminus P_3$. In dieser reduzierten Teilnehmermenge ist das Compartment C_1 minimal vertreten, alle Teilnehmer aus C_1 kommen also, ähnlich wie die Teilnehmer P_7 und P_8, in allen minimalen Mengen von $G \setminus P_3$ vor.

Dieser Sachverhalt gilt analog für die anderen Zeilen der Tabelle und ebenso für die Spalten und die Teilnehmer aus C_2.

Die Definition des erweiterten Tests auf Konsistenz für Compartment Schemes beruht auf den Beobachtungen des obigen Beispiels. Mit Hilfe dieses Tests können die Teilnehmer ihren Compartments zugeordnet werden.

Der erweiterte Test auf Konsistenz wird die folgenden drei Fragen (in dieser Reihenfolge) zu einer Teilnehmerkonfiguration G untersuchen:

a) Gibt es Teilnehmer, die in *allen* minimalen Mengen von G enthalten sind?

b) Gibt es Teilnehmer, die in *keiner* minimalen Menge von G vorkommen?

c) Gibt es in den echten Teilmengen von G Teilnehmer, die in allen minimalen Mengen dieser Teilmengen vorkommen?

Vor der Definition des erweiterten Tests auf Konsistenz werden die in dem Test verwendeten Prüfmengen und Prüfstrukturen eingeführt. Die Prüfmengen sind die unter c) genannten echten Teilmengen von *G*, die Prüfstrukturen enthalten die minimalen Mengen der Prüfmengen. Sie entsprechen den Spalten und Zeilen der Tabelle im obigen Beispiel.

4.7 Definition: PRÜFMENGEN

Sei $G \in \Gamma$ eine zulässige Teilnehmermenge eines Compartment Schemes. Die *Prüfmengen von G* sind die Teilmengen von *G*:

$$\{G_0, G_1, \ldots, G_g\} := \mathbf{P}(G)$$

Sie sind nach der Anzahl der enthaltenen Teilnehmer sortiert, dass heißt

$$|G_0| \le |G_1| \le \ldots \le |G_g|.$$

Ferner sei $g_i := \binom{|G|}{i}$ die Anzahl der *i*-elementigen Prüfmengen von *G* und

$$g := \sum_{i=0}^{|G|} g_i.$$

die Gesamtzahl der Prüfmengen von *G*.

4.8 Definition: PRÜFSTRUKTUREN

Sei $G \in \Gamma$ eine zulässige Teilnehmermenge eines Compartment Schemes. Seien $M_1, M_2, \ldots, M_m$ nach Definition 2.12 die minimalen Mengen von *G* und $\{G_0, G_1, \ldots, G_g\}$ nach Definition 4.7 die Prüfmengen zu *G*.

Dann heißt

$$\underline{M}_j := \left\{ M \in M \middle| M \cap G_j = \{\ \} \right\}$$
$$:= \left\{ \underline{M}_1^j, \underline{M}_2^j, \ldots, \underline{M}_{m_j}^j \right\}$$

Prüfstruktur von *G* zu G_j.

Eine Prüfstruktur *G* zu G_j hat die *Ordnung i*, wenn $|G_j| = i$ gilt ($i = 0, 1, \ldots, |G|$).

Für die Erzeugung der Prüfstruktur $\underline{M}_j = \{\underline{M}_1^j, \underline{M}_2^j, \ldots, \underline{M}_{m_j}^j\}$ werden demnach alle minimalen Mengen der Minimalstruktur von *G* ausgeschlossen, deren Durchschnitt mit

der Prüfmenge G_j nichtleer ist. Die Ordnung i einer Prüfstruktur $\underline{M}_j$ zu G_j gibt die Mächtigkeit der Prüfmenge G_j an.

Bevor mit diesen Prüfstrukturen der erweiterte Test auf Konsistenz definiert wird, soll das folgende Lemma zum Verständnis der Prüfstrukturen beitragen. Es wird darüber hinaus einige Beweise zum Test auf Konsistenz verkürzen.

4.9 Lemma:

Sei $G \in \Gamma$ nach Definition 2.9 eine zulässige Teilnehmermenge eines Compartment Schemes. Sei G' nach Definition 4.7 eine Prüfmenge zu G.

Sei ferner M nach Definition 2.12 die Minimalstruktur von G und M' die Minimalstruktur von $G \setminus G'$.

Schließlich sei $\underline{M}$ nach Definition 4.8 die Prüfstruktur von G zu G' mit $\underline{M} = \{M \in M \mid M \cap G' = \{\}\}$.

Dann gilt: $\underline{M} = M'$

Beweis:

a) Zu zeigen: $\underline{M} \subseteq M'$, es wird gezeigt: $M \in \underline{M} \Rightarrow M \in M'$
Sei $M \in \underline{M}$. Nach Definition 4.8 ist M eine minimale Menge von G, für die $M \cap G' = \{\}$ gilt. Daher ist M auch eine minimale Menge von $G \setminus G'$. Es gilt $M \in M'$.

b) Zu zeigen: $M' \subseteq \underline{M}$, es wird gezeigt: $M \in M' \Rightarrow M \in \underline{M}$
Sei $M \in M'$. Da M eine minimale Menge von $G \setminus G'$ ist, muss M auch eine minimale Menge von G sein. Ferner folgt $M \cap G' = \{\}$. Insgesamt gilt also $M \in \underline{M}$.

Das Lemma besagt, dass die beiden folgenden Wege zum gleichen Ergebnis führen:

- Die Minimalstruktur M von G wird berechnet, anschließend werden alle minimalen Mengen von M ausgeschlossen, deren Schnittmenge mit G' nichtleer ist. Das Ergebnis ist $\underline{M}$.
- Die Minimalstruktur M' von $G \setminus G'$ wird berechnet.

Anmerkung:
Die Prüfstrukturen in Definition 4.8 hätten auch als Minimalstrukturen von $G \setminus G'$ mit $G' \in \mathbf{P}(G)$ definiert werden können. Die Prüfstrukturen nach Definition 4.8 sind jedoch in der praktischen Umsetzung des im folgenden definierten Tests auf Konsistenz schneller zu berechnen.

Mit diesen Prüfstrukturen wird der erweiterte Test auf Konsistenz für Compartment Schemes durchgeführt.

4.10 Definition: ERWEITERTER TEST AUF KONSISTENZ (COMPARTMENT SCHEMES)

Sei $G \in \Gamma$ eine zulässige Teilnehmermenge eines Compartment Schemes. Seien $M_1, M_2, \ldots, M_m$ die Mengen der Minimalstruktur M von G mit $|M| > 1$.

Der *erweiterte Test auf Konsistenz* besteht aus drei Teilen:

Teil I:
Aus der Minimalstruktur M werden zwei Ergebnismengen gebildet:

$$E'^{0}_{\mathrm{M}} := \{ P \in G \mid P \in M_i \text{ für } \textit{alle } i = 1, 2, \ldots, m)\}$$

$$E_{\mathrm{N}} := \{ P \in G \mid P \notin M_i \text{ für } \textit{alle } i = 1, 2, \ldots, m)\}$$

Der erweiterte Test auf Konsistenz heißt *durchführbar*, wenn

$$E'^{0}_{\mathrm{M}} = \{\}$$

gilt.

Teil II:
Für jede minimale Menge M_i werden die Mengen B_i und K_i wie folgt gebildet:

$$B_i := \left\{ B \in B \middle| \left(\alpha_K \left(M_i \right), B \right) \in \beta \right\}$$

$$K_i := \left\{ K \in K \middle| \kappa(b) = K \text{ für alle } b \in B_i \right\}$$

Die Menge G besteht den *erweiterten Test auf Konsistenz* genau dann, wenn jedes K_i aus genau einem Element besteht und alle diese Elemente gleich sind.

Teil III:

Schritt 1:
Für die Prüfstrukturen der Ordnung 1 werden die Ergebnismengen $E^1_{\mathrm{M}}, E^2_{\mathrm{M}}, \ldots, E^{|G|}_{\mathrm{M}}$ wie folgt gebildet:

$$E'^{1}_{\mathrm{M}} := \left\{ P \in G \middle| P \notin M \text{ für alle } M \in \underline{M}_1 \right\} \setminus \left(G_1 \cup E_{\mathrm{N}} \right)$$

$$\vdots$$

$$E'^{|G|}_{\mathrm{M}} := \left\{ P \in G \middle| P \notin M \text{ für alle } M \in \underline{M}_{|G|} \right\} \setminus \left(G_{|G|} \cup E_{\mathrm{N}} \right)$$

$$E^{1}_{\mathrm{M}} := \begin{cases} E'^{1}_{\mathrm{M}} \cup G_1 & \text{für } E'^{1}_{\mathrm{M}} \neq \{\,\} \\ \{\,\} & \text{für } E'^{1}_{\mathrm{M}} = \{\,\} \end{cases}$$

$$\vdots$$

$$E^{|G|}_{\mathrm{M}} := \begin{cases} E'^{|G|}_{\mathrm{M}} \cup G_{|G|} & \text{für } E'^{|G|}_{\mathrm{M}} \neq \{\,\} \\ \{\,\} & \text{für } E'^{|G|}_{\mathrm{M}} = \{\,\} \end{cases}$$

Schritt 2:
Sei c_k (für $k = 0, 1, \ldots, |G|$) die Anzahl aller Prüfstrukturen einer Ordnung kleiner gleich k, d.h. mit den Bezeichnungen aus Definition 4.7

$$c_k = \sum_{i=0}^{k} g_i = \sum_{i=0}^{k} \binom{|G|}{i} \text{ für } k = 0, 1, \ldots, |G|.$$

Für die nichtleeren Prüfstrukturen der Ordnung $k = 1, 2, \ldots, |G|$ werden sukzessiv die Ergebnismengen derselben Ordnung wie folgt gebildet:

$$E_{c_{k-1}} := \left\{ P \in G \,\middle|\, P \in M \text{ für alle } M \in \underline{M}_{c_{k-1}} \right\} \setminus R_k$$
$$\vdots$$
$$E_{c_k - 1} := \left\{ P \in G \,\middle|\, P \in M \text{ für alle } M \in \underline{M}_{c_k - 1} \right\} \setminus R_k$$

Die Mengen R_k enthalten alle Teilnehmer, die in einer der zuvor gebildeten Ergebnismengen vorkommen. Es gilt:

$$R_1 = E_{\mathrm{N}} \cup E_{\mathrm{M}}^{1} \cup \ldots \cup E_{\mathrm{M}}^{|G|}$$

und für $k \geq 2$

$$R_k := E_{\mathrm{N}} \cup E_{\mathrm{M}}^{1} \cup \ldots \cup E_{\mathrm{M}}^{|G|} \cup \left(\bigcup_{j=1}^{c_{k-1}-1} E_j \right)$$

Aus diesen Mengen werden die Vereinigungsmengen E_{C}^{j} $(1 \leq j \leq g)$ wie folgt gebildet:

$$E_{\mathrm{C}}'^{1} := \bigcup_{\substack{E \in \{E_2, \ldots, E_g\} \\ E \cap E_1 \neq \{\}}} E$$
$$\vdots$$
$$E_{\mathrm{C}}'^{j} := \bigcup_{\substack{E \in \{E_1, \ldots, E_{j-1}, E_{j+1}, \ldots, E_g\} \\ E \cap E_j \neq \{\}}} E$$
$$\vdots$$
$$E_{\mathrm{C}}'^{g} := \bigcup_{\substack{E \in \{E_1, \ldots, E_{g-1}\} \\ E \cap E_g \neq \{\}}} E$$

$$E_C^1 := \begin{cases} E_C'^1 \cup E_1 & \text{wenn } E_C'^1 \neq \{\ \} \\ \{\ \} & \text{wenn } E_C'^1 = \{\ \} \end{cases}$$

$$\vdots$$

$$E_C^g := \begin{cases} E_C'^g \cup E_g & \text{wenn } E_C'^g \neq \{\ \} \\ \{\ \} & \text{wenn } E_C'^g = \{\ \} \end{cases}$$

Anmerkung:
Der Test erfordert viele Einzelschritte. Für die praktische Anwendung wird der Test noch dahingehend untersucht werden müssen, welche Schritte sich durch Optimierungen erübrigen.

Der erweiterte Test auf Konsistenz ist in Abbildung 20 (Seite 83) dargestellt. Dort sind auch die Zusammenhänge der einzelnen Mengen, die während des Tests erzeugt werden, ablesbar. Diese Zusammenhänge werden durch die folgenden Sätze und Lemmas geklärt. Darüber hinaus enthält Kapitel 4.3 Beispiele, welche die Bedeutung der einzelnen Menge veranschaulichen.

Zunächst werden die Mengen E_N und $E_M'^0$, die in Teil I des Testes berechnet werden, untersucht.

4.11 Satz:

Sei $G \in \Gamma$ eine zulässige Teilnehmermenge eines Compartment Schemes. Der erweiterte Test auf Konsistenz werde nach Definition 4.10 durchgeführt.

Dann gilt für die in Teil I des Tests berechnete Menge E_N:

$$P \in E_N \;\Leftrightarrow\; P \in G \cap C_k \text{ mit } |G \cap C_k| < t_k$$

Beweis:

Zu zeigen ist:

a) $P \in E_N \;\Rightarrow\; P \in G \cap C_k$ mit $|G \cap C_k| < t_k$, es wird gezeigt:
Wenn ein Teilnehmer P aus einem Compartment C_k stammt, dass mit *mindestens* t_k Teilnehmern vertreten ist, dann ist P *nicht* in E_N enthalten.

b) $P \in G \cap C_k$ mit $|G \cap C_k| < t_k \;\Rightarrow\; P \in E_N$, es wird gezeigt:
Wenn ein Teilnehmer P aus einem Compartment C_k stammt, dass mit weniger als t_k Teilnehmern vertreten ist, dann ist P in E_N enthalten.

Zu a):
Sei $P \in G \cap C_k$ mit $|G \cap C_k| \geq t_k$.

Da nach Definition 4.10 mehrere minimale Mengen von G bestehen ($|M| > 1$), müssen (mindestens) t Compartments $C_{i_1}, C_{i_2}, \ldots, C_{i_t}$ mit mindestens $t_{i_1}, t_{i_2}, \ldots, t_{i_t}$ Teilnehmern in G enthalten sein. Sei $C_k \in \{C_{i_1}, C_{i_2}, \ldots, C_{i_t}\}$. Das ist möglich, da $|G \cap C_k| \geq t_k$ gilt.

Sei ferner M eine Menge, die von den Compartments $C_{i_1}, C_{i_2}, \ldots, C_{i_t}$ genau $t_{i_1}, t_{i_2}, \ldots, t_{i_t}$ Teilnehmer enthält. Die Teilnehmer von M seien so gewählt, dass $P \in M$ gilt. M ist nach Definition 2.11 eine minimale Menge, da M durch Entfernen eines Teilnehmers unzulässig wird. Es gibt folglich eine minimale Menge M mit $P \in M$.

E_N ist nach Definition 4.10 die Menge aller Teilnehmer, die in keiner der minimalen Mengen von G enthalten sind. Daher ist P nicht in E_N enthalten.

Zu b):
Der Beweis erfolgt indirekt:
P sei aus einem Compartment C_k, dass mit weniger als t_k Teilnehmern vertreten ist, und P sei nicht in E_N enthalten.

Da $P \notin E_N$ gilt, gibt es nach Definition 4.10 mindestens eine minimale Menge M mit $P \in M$.

Sei $M' = M \setminus P$. Dann muss M' nach Definition 2.9 zulässig sein, da P nach Voraussetzung ($|G \cap C_k| < t_k$) nicht an der Rekonstruktion beteiligt ist. Folglich ist M nach Definition 2.11 keine minimale Menge, was ein Widerspruch ist.

In E_N sind nach Satz 4.11 alle Teilnehmer enthalten, die nicht zur Rekonstruktion beitragen. Dafür gibt es im wesentlichen zwei mögliche Gründe:

- Aus dem Compartment des Teilnehmers nehmen nicht genügend Teilnehmer an der Rekonstruktion teil oder
- der Teilnehmer hat nicht das Teilgeheimnis angegeben, das ihm zugeteilt wurde, er hat betrogen.

Der folgende Satz klärt die Bedeutung der Menge E'^{0}_{M}, die ebenfalls in Teil I des erweiterten Testes auf Konsistenz berechnet wird. Dabei werden zwei Fälle unterschieden. Es seien

- genau t Compartments oder
- mehr als t Compartments

mit zur Rekonstruktion ausreichender Teilnehmerzahl in G enthalten (t ist nach Definition 2.9 die Schwelle der für die Rekonstruktion benötigten Compartments).

4.12 Satz:

Sei $G \in \Gamma$ eine zulässige Teilnehmermenge eines Compartment Schemes (nach Definition 2.9). Der erweiterte Test auf Konsistenz werde nach Definition 4.10 durchgeführt.

a) Sei $|G \cap C_k| \geq t_k$ für $k = i_1, i_2, \ldots, i_t$ und $|G \cap C_k| < t_k$ für $k \neq i_1, i_2, \ldots, i_t$.

Dann gilt:

$$P \in E'^0_M \Leftrightarrow P \in G \cap C_k \text{ mit } |G \cap C_k| = t_k$$

b) Sei $|G \cap C_k| \geq t_k$ für $k = i_1, i_2, \ldots, i_{t'}$ und $|G \cap C_k| < t_k$ für $k \neq i_1, i_2, \ldots, i_{t'}$ mit $t' > t$.

Dann gilt:

$$E'^0_M = \{\ \}$$

Beweis:

Zu a):
An der Rekonstruktion seien genau t Compartments mit jeweils ausreichender Teilnehmerzahl beteiligt: Zu zeigen ist:

i) $P \in E'^0_M \Rightarrow P \in G \cap C_k$ mit $|G \cap C_k| = t_k$, es wird gezeigt:
Wenn ein Compartment C_k nach Definition 2.10 *nicht* minimal in G ist (das heißt $|G \cap C_k| \neq t_k$), dann sind *keine* Teilnehmer aus $G \cap C_k$ in E'^0_M enthalten.

ii) $P \in G \cap C_k$ mit $|G \cap C_k| = t_k \Rightarrow P \in E'^0_M$, es wird gezeigt:
Wenn ein Compartment C_k in G nach Definition 2.10 minimal ist (das heißt $|G \cap C_k| = t_k$), dann sind alle Teilnehmer aus $G \cap C_k$ in E'^0_M enthalten.

Zu i):
Sei zunächst $|G \cap C_k| < t_k$.
Dann sind alle Teilnehmer aus $G \cap C_k$ nach Satz 4.11 in E_N enthalten. Folglich beinhaltet nach Definition 4.10 keine minimale Menge einen Teilnehmer aus $G \cap C_k$.

E'^0_M ist die Menge aller Teilnehmer, die in allen minimalen Mengen von G vorkommen. Daher ist in E'^0_M kein Teilnehmer aus $G \cap C_k$ enthalten.

Sei nun $|G \cap C_k| > t_k$, der Beweis erfolgt indirekt:
Sei $P \in G \cap C_k$ und $P \in E'^0_M$.
Da $P \in E'^0_M$ gilt, muss P nach Definition 4.10 in allen minimalen Mengen von G enthalten sein. Sei $G' = G \setminus P$. Da $|G \cap C_k| > t_k$ gilt und G eine zulässige Teilnehmermenge ist, folgt: $|G' \cap C_k| \geq t_k$ und G' ist nach Definition 2.9 ebenfalls zulässig.

Es gibt also mindestens eine minimale Menge $M' \subseteq G'$ mit $P \notin M'$, was ein Widerspruch zu $P \in E'^0_M$ ist.

Zu ii):
Sei $|G \cap C_k| = t_k$ und $P \in G \cap C_k$..

Da nach Voraussetzung genau t Compartments an der Rekonstruktion teilnehmen, muss jedes Compartment, also auch C_k, in jeder minimalen Menge vertreten sein. Da C_k minimal ist, muss sich, damit C_k in jeder minimalen Menge vertreten ist, jeder Teilnehmer aus $G \cap C_k$ in jeder minimalen Menge befinden. Folglich ist nach Definition 4.10 jeder Teilnehmer aus $G \cap C_k$ in E'^0_M enthalten.

Zu b):
An der Rekonstruktion seien mehr als t Compartments mit jeweils ausreichender Teilnehmerzahl beteiligt: Zu zeigen ist: $E'^0_M = \{\ \}$

Sei $P \in G \cap C_k$. Da mehr als t Compartments mit ausreichender Teilnehmerzahl vorhanden sind, gibt es eine zulässige Teilnehmermenge $M' := C_{i_1} \cup C_{i_2} \cup \ldots \cup C_{i_t}$ mit $M' \cap C_k = \{\}$. Ferner existiert (mindestens) eine minimale Menge $M \subseteq M'$ von G mit $P \notin M$.

E'^0_M ist nach Definition 4.10 die Menge aller Teilnehmer, die in allen minimalen Mengen von G vorkommen. Daher gilt für jeden Teilnehmer P aus $G \cap C_k$: $P \notin E'^0_M$.

Nach Satz 4.12 gibt es für zulässige Teilnehmermengen G zwei Situationen, in denen $E'^0_M = \{\ \}$ gilt:

- Alle zur Rekonstruktion benötigten Compartments C_k sind mit mehr als t_k Teilnehmern in G vertreten, oder
- es gibt mehr als t Compartments C_k mit mindestens t_k Teilnehmern in G.

Die Überlegungen in Kapitel 4.2.2 haben ergeben, dass dies genau die beiden Voraussetzungen sind, unter denen eine Konsistenzaussage bezüglich der Glaubwürdigkeit eines rekonstruierten Teilgeheimnisses möglich ist. Die Aussage aus Definition 4.10, der Test sei durchführbar, wenn $E'^0_M = \{\ \}$ gilt, ist daher plausibel.

Der folgende Satz zeigt, dass, wenn der Test auf Konsistenz durchführbar ist, alle Teilnehmer aus minimalen Compartments in den Ergebnismengen E'^i_M ($i = 1, 2, \ldots, |G|$), die in Teil III des erweiterten Tests auf Konsistenz berechnet werden, enthalten sind.

4.13 Satz:

Sei $G \in \Gamma$ eine zulässige Teilnehmermenge eines Compartment Schemes. Der erweiterte Test auf Konsistenz werde nach Definition 4.10 durchgeführt und es gelte $E'^0_M = \{\}$.

Dann gilt für die in Teil III (Schritt 1) des Tests berechneten Mengen E'^i_M:

$$P \in E'^i_M \text{ für ein } i \in \{1, 2, \ldots, |G|\} \quad \Leftrightarrow \quad P \in G \cap C_k \text{ mit } |G \cap C_k| = t_k$$

Beweis:
Nach Satz 4.12 folgt aus $E'^{0}_{M} = \{\}$, dass

1) entweder genau t Compartments an der Rekonstruktion beteiligt sind, dann muss für jedes beteiligte Compartment $|G \cap C_k| \geq t_k + 1$ gelten, oder
2) mindestens $t + 1$ Compartments an der Rekonstruktion mitwirken.

Die zu beweisende Äquivalenz wird für diese beiden Fälle betrachtet:

Zu 1):
Es gelte zunächst für die t an der Rekonstruktion beteiligten Compartments:
$|G \cap C_k| \geq t_k + 1$

Die rechte Seite der zu beweisenden Äquivalenz ist dann für keinen Teilnehmer P erfüllt. Das folgende Argument zeigt, dass auch die linke Seite für keinen Teilnehmer erfüllt ist:

Eine Menge E'^{i}_{M} enthält nach Definition 4.10 alle Teilnehmer, die in keiner der minimalen Mengen einer Prüfstruktur der Ordnung 1 vorkommen. Mit anderen Worten (nach Lemma 4.9) enthält eine Menge E'^{i}_{M} jeden Teilnehmer P, der in keiner minimalen Menge von $G' := G \setminus X$ vorkommt (für ein $X \in G$ mit $X \neq P$).

Sei E'_N die nach Definition 4.10 für die Teilnehmermenge G' gebildete Menge E_N. Dann gilt $P \in E'_N$, da P in keiner minimalen Menge von G' vorkommt. Daraus folgt nach Satz 4.11: $P \in G' \cap C_k$ mit $|G' \cap C_k| < t_k$ und daher

$$|G \cap C_k| = |\{G' \cup X\} \cap C_k| < t_k + 1.$$

Das ist ein Widerspruch zur Voraussetzung.

Zu 2):
Zu zeigen: Wenn mehr als t Compartments in G enthalten sind, dann gilt:

a) $P \in E'^{i}_{M} \Rightarrow P \in G \cap C_k$ mit $|G \cap C_k| = t_k$, es wird gezeigt:
Wenn ein Compartment C_k in G *nicht* minimal ist (das heißt nach Definition 2.10: $|G \cap C_k| \neq t_k$), dann sind in *keiner* Menge E'^{i}_{M} Teilnehmer aus $G \cap C_k$ enthalten.

b) $P \in G \cap C_k$ mit $|G \cap C_k| = t_k \Rightarrow P \in E'^{i}_{M}$, es wird gezeigt:
Wenn ein Compartment C_k in G nach Definition 2.10 minimal ist, dann sind die Teilnehmer aus $G \cap C_k$ in (mindestens) einer Menge E'^{i}_{M} enthalten.

Zu a)
i) Sei zunächst $|G \cap C_k| < t_k$.
Dann sind alle Teilnehmer aus $G \cap C_k$ nach Satz 4.11 in E_N enthalten. Da nach Definition 4.10 die Mengen E'^{i}_{M} keine Teilnehmer aus E_N beinhalten, sind in keiner Menge E'^{i}_{M} Teilnehmer aus $G \cap C_k$ enthalten.

ii) Sei nun $|G \cap C_k| > t_k$, der Beweis erfolgt indirekt:

Sei $P \in G \cap C_k$ und $P \in E'^{\,i}_{\mathrm{M}}$ für ein $i \in \{1, 2, \ldots, |G|\}$.

Da $P \in E'^{\,i}_{\mathrm{M}}$ gilt, existiert nach Definition 4.10 eine Prüfstruktur der Ordnung 1, welche nur minimale Mengen beinhaltet, in denen P nicht vorkommt. Folglich gibt es nach Lemma 4.9 ein $X \in G$ mit $X \neq P$, so dass gilt:

$$\text{Sei } M \text{ eine minimale Menge von } G' := G \setminus X \Rightarrow P \notin M.$$

Da $|G \cap C_k| > t_k$ gilt, folgt $|G' \cap C_k| = |\{G \setminus X\} \cap C_k| \geq t_k$. Da also in G' mindestens t_k Teilnehmer aus C_k enthalten sind, existiert eine minimale Menge $M' \subseteq G'$, die Teilnehmer aus $G' \cap C_k$ und insbesondere $P \in G \cap C_k$ beinhaltet. Das ist ein Widerspruch.

Zu b):
Sei $P \in G \cap C_k$ und $|G \cap C_k| = t_k$.
Sei ferner $G' := G \setminus X$ mit $X \in G \cap C_k$ und $X \neq P$. Es gilt:

$$|G' \cap C_k| = t_k - 1 < t_k$$

Für G' gibt es keine minimale Menge, die P enthält, da aus dem Compartment C_k keine t_k Teilnehmer in G' enthalten sind. Die Prüfstruktur von G zu X enthält folglich nach Lemma 4.9 keine minimalen Mengen, in denen P vorkommt. Nach Definition 4.10 gilt daher $P \in E'^{\,i}_{\mathrm{M}}$ für mindestens ein $i \in \{1, 2, \ldots, |G|\}$.

Aus den Sätzen 4.12 und 4.13 folgt, dass alle Teilnehmer aus minimalen Compartments in mindestens einer der Mengen $E'^{\,i}_{\mathrm{M}}$ enthalten sind ($i \in \{1, 2, \ldots, |G|\}$). Wenn der Test nach Definition 4.10 durchführbar ist (d.h. $E'^{\,0}_{\mathrm{M}} = \{\}$), dann können diese Teilnehmer ihren Compartments zugeordnet werden. Das wird durch das nächste Lemma und den darauffolgenden Satz gezeigt.

4.14 Lemma:

Sei $G \in \Gamma$ eine zulässige Teilnehmermenge eines Compartment Schemes. Der erweiterte Test auf Konsistenz werde nach Definition 4.10 durchgeführt und es gelte $E'^{\,0}_{\mathrm{M}} = \{\}$.

Dann sind in einer der in Teil III (Schritt 1) des Tests berechneten nichtleeren Menge $E'^{\,i}_{\mathrm{M}}$ genau $t_k - 1$ Teilnehmer eines Compartments C_k und keine Teilnehmer anderer Compartments enthalten.

Beweis:
Nach Satz 4.12 folgt aus $E'^{\,0}_{\mathrm{M}} = \{\}$, dass in jedem Compartment mindestens ein Teilnehmer oder mindestens ein Compartment mehr in G enthalten ist, als zur Rekonstruktion benötigt wird. Wie bereits im Beweis zu Satz 4.13 gezeigt, muss für die nichtleeren $E'^{\,i}_{\mathrm{M}}$ nur der letztere Fall (d.h. mindestens ein Compartment „zu viel“) betrachtet werden.

Ebenfalls analog zum Beweis zu Satz 4.13 wird eine Teilnehmermenge $G' := G \setminus X$ betrachtet. Für einen Teilnehmer $P \neq X$, der in einer Ergebnismenge E'^{i}_{M} enthalten ist, gilt dann nach Definition 4.10:

- P kommt in keiner minimalen Menge von G' vor und
- ist nicht in E_N enthalten.

Sei C_x das Compartment, zu dem X gehört ($X \in G \cap C_x$) und E'^{x}_{M} die Ergebnismenge zu X. Zu zeigen ist:

a) In den nichtleeren E'^{i}_{M} kommen nur Teilnehmer *eines* Compartments vor. Es wird gezeigt, dass in E'^{x}_{M} keine Teilnehmer aus einem Compartment $C_i \neq C_x$ enthalten sein können.

b) In den nichtleeren E'^{i}_{M} sind genau t_k - 1 Teilnehmer eines Compartments C_k enthalten. Es wird gezeigt, dass in E'^{x}_{M}, sofern $E'^{x}_{M} \neq \{\}$, genau t_x - 1 Teilnehmer aus C_x enthalten sind.

Zu a):
Da mehr als t Compartments an der Rekonstruktion teilnehmen, ist $G' = G \setminus X$ eine zulässige Teilnehmermenge. Im folgenden wird ein Teilnehmer P betrachtet mit $P \notin C_x$.

i) P trage in G' nicht zur Rekonstruktion bei.
Dann trägt $P \notin C_x$ auch in $G = G' \cup X$ nicht zur Rekonstruktion bei. Daher ist P nach Satz 4.11 in E_N enthalten. Nach Definition 4.10 gilt dann $P \notin E'^{x}_{M}$.

ii) P trage in G' zur Rekonstruktion bei.
Dann gibt es eine minimale Menge von G', die P enthält. Es gilt ebenfalls nach Definition 4.10: $P \notin E'^{x}_{M}$.

Da also insgesamt kein Teilnehmer $P \notin C_x$ in E'^{x}_{M} enthalten ist, können in E'^{x}_{M} nur Teilnehmer aus C_x enthalten sein.

Zu b):
i) Sei $|G \cap C_x| < t_x$
Dann tragen die Teilnehmer aus dem Compartment C_x in G und G' nicht zur Rekonstruktion bei. Folglich haben G und $G' = G \setminus X$ (mit $X \in G \cap C_x$) dieselbe Minimalstruktur. Es gibt also keine Teilnehmer, die einerseits in keiner minimalen Menge von G' und andererseits nicht in E_N enthalten sind.

Nach Definition 4.10 gilt dann $E'^{x}_{M} = \{\}$, und der Satz ist für $|G \cap C_x| < t_x$ bewiesen.

ii) Sei $|G \cap C_x| > t_x$
Dann gilt $|G' \cap C_x| \geq t_x$, das heißt die Teilnehmer aus dem Compartment C_x tragen in G' zur Rekonstruktion bei. Daher kommt jeder Teilnehmer (abgesehen von X) aus $G' \cap C_x$ in mindestens einer minimalen Menge von G' vor.

Nach Definition 4.10 gilt dann $E'^{x}_{M} = \{\}$, und der Satz ist für $|G \cap C_x| > t_x$ bewiesen.

iii) Sei $|G \cap C_x| = t_x$
Dann trägt das Compartment C_x in G zur Rekonstruktion bei, in G' jedoch nicht. Jeder Teilnehmer aus $G' \cap C_x$ kommt daher einerseits in keiner minimalen Menge von G' und andererseits nicht in E_N vor. Folglich sind nach Definition 4.10 die $t_x - 1$ Teilnehmer aus $\{G \setminus X\} \cap C_x$ in der Ergebnismenge E'^{x}_{M} von G zu X enthalten.

Der Satz gilt also auch für $|G \cap C_x| = t_x$.

4.15 Satz:

Sei $G \in \Gamma$ eine zulässige Teilnehmermenge eines Compartment Schemes. Der erweiterte Test auf Konsistenz werde nach Definition 4.10 durchgeführt und es gelte $E'^{0}_{M} = \{\}$.

Dann sind in den in Teil III (Schritt 1) des Tests berechneten nichtleeren Mengen E^{i}_{M} alle Teilnehmer eines Compartments und nur Teilnehmer eines Compartments enthalten.

Beweis:
Analog zum Beweis zu Lemma 4.14 wird eine Teilnehmermenge $G' := G \setminus X$ betrachtet. Sei C_x das Compartment, zu dem X gehört ($X \in G \cap C_x$) und E'^{x}_{M} die Ergebnismenge zu X.

Aus dem Beweis zu Lemma 4.14 wird ersichtlich, dass die Ergebnismenge E'^{x}_{M}, wenn sie nichtleer ist, die $t_x - 1$ Teilnehmer aus $\{G \setminus X\} \cap C_x$ enthält. Nach Definition 4.10 wird aus dieser Ergebnismenge (wenn sie nichtleer ist), durch Vereinigung mit X die Menge E^{x}_{M} gebildet. Daraus folgt $E^{x}_{M} = G \cap C_x$.

Anmerkung:
Nach Satz 4.13 werden nur die in G minimalen Compartments in den Ergebnismengen E^{i}_{M} rekonstruiert.

Es folgen einige Sätze und Lemmas, mit deren Hilfe dann die Bedeutung der Vereinigungsmengen $E^{1}_{C}, \ldots, E^{g}_{C}$ in Satz 4.20 bewiesen wird.

Zuerst wird durch einige Lemmas die Bedeutung der Ergebnismengen E_k, die im dritten Teil (Schritt 2) des Tests auf Konsistenz gebildet werden, geklärt. In diesem Teil des Tests werden nacheinander die Prüfstrukturen wachsender Ordnung betrachtet. Teilnehmer, die in allen minimalen Mengen einer solchen Prüfstruktur enthalten sind, bilden die Ergebnismengen E_k. Nach Lemma 4.9 ist das gleichbedeutend damit, dass ein Teilnehmer in jeder minimalen Menge der Minimalstruktur einer Teilnehmermenge $G' := G \setminus X$ ($X \subseteq G$) enthalten ist.

Das folgende Lemma sagt aus, dass ein Teilnehmer P nur dann in einer der Ergebnismengen enthalten ist, wenn er aus einem Compartment stammt, das in der zugehörigen, um X reduzierten Teilnehmermenge G' minimal ist.

4.16 Lemma:

Sei $G \in \Gamma$ eine zulässige Teilnehmermenge eines Compartment Schemes. Der erweiterte Test auf Konsistenz werde nach Definition 4.10 durchgeführt.

Sei E_k eine der in Teil III des Testes gebildeten Ergebnismengen und $\underline{M}$ nach Definition 4.7 die zugehörige Prüfstruktur.

Ferner sei $G' := G \setminus X$ diejenige Teilnehmermenge, für welche die Prüfstruktur $\underline{M}$ nach Lemma 4.9 die Minimalstruktur enthält (d.h. $\underline{M} = \{M \in M \mid M \cap X = \{\}\}$, wobei M die Minimalstruktur von G ist) und sei $P \in G'$.

Dann gilt:

$$P \in E_k \;\Rightarrow\; P \in C_j \text{ mit } |G' \cap C_j| = t_j$$

Beweis:
Zu zeigen:
Wenn P in einer Ergebnismenge E_k enthalten ist, dann stammt P aus einem Compartment, das in der um X reduzierten Teilnehmermenge G' nach Definition 2.10 minimal ist.

Sei $P \in E_k$. Dann ist nach Definition 4.10 der Teilnehmer P in allen minimalen Mengen von G' enthalten.

Sei $P \in C_j$ mit $|G' \cap C_j| < t_j$:
Dann trägt C_j nicht zur Rekonstruktion bei. Daher ist kein Teilnehmer aus C_j in einer minimalen Menge von G' vertreten. Das ist ein Widerspruch zu $P \in E_k$ und es folgt $|G' \cap C_j| \geq t_j$.

Sei $P \in C_j$ mit $|G' \cap C_j| > t_j$:
Sei $J := G' \setminus P$. J rekonstruiert dasselbe Geheimnis wie G', da $|G' \cap C_j| > t_j$. Es gibt demnach mindestens eine minimale Menge $M \subseteq J$ von G', die P nicht enthält. Das ist ein Widerspruch und es folgt $|G' \cap C_j| \leq t_j$

Insgesamt folgt: $|G' \cap C_j| = t_j$

Anmerkung:
Die Umkehrung des Satzes gilt nicht. Gegenbeispiele lassen sich leicht mit mehr als t an der Rekonstruktion beteiligten Compartments konstruieren.

Das nun folgende Lemma klärt die Struktur der Ergebnismengen bereits weitgehend auf. Es zeigt, dass zwei Teilnehmer, die in derselben Ergebnismenge E_k enthalten sind, zu demselben Compartment gehören.

4.17 Lemma:

Sei $G \in \Gamma$ eine zulässige Teilnehmermenge eines Compartment Schemes. Der erweiterte Test auf Konsistenz werde nach Definition 4.10 durchgeführt, es gelte $E'^{0}_{M} = \{\}$. Dann gilt:

Wenn zwei Teilnehmer P und P' in einer Menge E_k enthalten sind,
dann gehören sie zu demselben Compartment.

Beweis:
Der Beweis erfolgt indirekt:
Sei $P, P' \in E_k$ und $P \in C_i$, $P' \in C_j$ mit $i \neq j$.
Es wird gezeigt, dass P und P' unter dieser Voraussetzung bereits in einer Ergebnismenge einer geringeren Ordnung als der von E_k enthalten sein müssen. Das ist dann ein Widerspruch.

Da $P, P' \in E_k$ gilt, sind P und P' nach Definition 4.10 in keiner Menge E^{i}_{M} enthalten (da $R_1 = E_N \cup E^{1}_{M} \cup \ldots \cup E^{|G|}_{M}$ und $E_k \cap R_1 = \{\}$). Die Compartments C_i und C_j sind daher nach den Sätzen 4.12 und 4.13 nicht minimal in G.

Sei $\underline{M}_k$ nach Definition 4.7 die zu E_k gehörende Prüfstruktur. Ferner sei $G' := G \setminus X$ mit $X \subseteq G$ diejenige Teilnehmermenge, für die $\underline{M}_k$ nach Lemma 4.9 die Minimalstruktur enthält (d.h. $\underline{M}_k = \{M \in M \mid M \cap X = \{\}\}$, M sei die Minimalstruktur von G). Da die Compartments C_i und C_j nicht minimal in G sind und nach Lemma 4.16 in G' minimal sein müssen, gilt für die Ordnung n der Prüfstruktur $\underline{M}_k$:

$$n = |X| \geq 2.$$

Da die Teilnehmer P und P' in der Ergebnismenge E_k enthalten sind,

- kommen sie in allen minimalen Mengen von $\underline{M}_k$ (bzw. G') vor und
- es gilt $P, P' \notin R_n$.

$P, P' \notin R_n$ wiederum bedeutet nach Definition 4.10 sowie den Sätzen 4.11, 4.12 und 4.13, dass die Teilnehmer P und P'

- nicht in einem Compartment enthalten sind, das *nicht* an der Rekonstruktion beteiligt ist ($P \notin E_N$),
- nicht aus einem in G minimalen Compartment stammen ($P \notin E^{i}_{M}$) und
- nicht in einer Ergebnismenge einer Ordnung kleiner als n enthalten sind.

Im folgenden wird gezeigt, dass die letzte der obigen Bedingungen nicht erfüllt ist. Sei $J := G' \cup P''$ mit $P'' \in C_i$ und $P'' \notin G'$. Ein solches P'' existiert, da C_i nach Lemma 4.16 in G' minimal und in G (wegen $P \notin E^{i}_{M}$, s.o.) nicht minimal ist.

Die Minimalstruktur von J ist nach Definition 4.7 eine Prüfstruktur der Ordnung n-1. Jede minimale Menge von J enthält $P' \in C_j$, da

- nach Voraussetzung jede minimale Menge von G' den Teilnehmer P' enthält,
- J dieselbe Anzahl von Teilnehmern aus C_j enthält wie G' (und $P' \in C_j$ gilt) und
- J dieselbe Anzahl von Compartments enthält wie G'.

Das bedeutet aber, dass P' bereits in einer Ergebnismenge der Ordnung kleiner als n enthalten sein muss. Das ist ein Widerspruch.

Ein Teilnehmer P ist nach Definition 4.10 genau dann in E_k enthalten, wenn er in jeder minimalen Menge von $G' := G \setminus X$ (mit $X \subseteq G$) vorkommt. Das nächste Lemma liefert notwendige und hinreichende Voraussetzungen für das Enthaltensein eines Teilnehmers in jeder minimalen Menge einer zulässigen Teilnehmermenge G'.

4.18 Lemma:

Sei $G' \in \Gamma$ eine zulässige Teilnehmermenge eines Compartment Schemes.

Ein Teilnehmer P ist genau dann in jeder nach Definition 2.11 minimalen Menge von G' enthalten, wenn er

- aus einem in G' minimalen Compartment C_j stammt und
- genau t Compartments an der Rekonstruktion teilnehmen.

t ist nach Definition 2.9 die Anzahl der für die Rekonstruktion benötigten Compartments.

Beweis:
Sei M die Minimalstruktur von G'. Da $G' \in \Gamma$ eine zulässige Teilnehmermenge des Compartment Schemes ist, gilt $|M| > 0$. Es gibt also mindestens eine minimale Menge.

Sei $P \in G' \cap C_j$. Zu zeigen:

a) P ist in jeder minimalen Menge enthalten $\Rightarrow$
$P \in G' \cap C_j$ mit $|G' \cap C_j| = t_j$ und
$|G' \cap C_k| \geq t_k$ für $k = i_1, i_2, \ldots, i_t$ und $|G' \cap C_k| < t_k$ für $k \neq i_1, i_2, \ldots, i_t$

b) $P \in G' \cap C_j$ mit $|G' \cap C_j| = t_j$ und
$|G' \cap C_k| \geq t_k$ für $k = i_1, i_2, \ldots, i_t$ und $|G' \cap C_k| < t_k$ für $k \neq i_1, i_2, \ldots, i_t \Rightarrow$
P ist in jeder minimalen Menge enthalten.

Zu a)
Nach Definition 4.10 folgt aus der Voraussetzung, nämlich dass der Teilnehmer P in jeder minimalen Menge von G' vorkommt, dass P in (mindestens) einer Ergebnismenge E'^{0}_{M} enthalten ist. Nach Satz 4.12 folgt aus $P \in E'^{0}_{M}$ die zu beweisende Aussage.

Zu b)
Da genau t Compartments an der Rekonstruktion teilnehmen, muss jedes Compartment in jeder minimalen Menge vertreten sein. Da ferner $P \in G' \cap C_j$ mit $|G' \cap C_j| = t_j$ gilt, muss jeder Teilnehmer aus $G \cap C_j$ in jeder minimalen Menge enthalten sein.

Der letzte Schritt im dritten Teil des erweiterten Tests auf Konsistenz nach Definition 4.10 besteht darin, die Ergebnismengen, deren Schnittmenge nichtleer ist, zu den Mengen $E_C^1, \ldots, E_C^g$ zu vereinen. Da nach Lemma 4.17 nur Teilnehmer eines Compartments in den Ergebnismengen E_k enthalten sind, liegt die Annahme nahe, dass in diesen Vereinigungsmengen die Teilnehmer aus G, sortiert nach ihrer Zugehörigkeit zu den einzelnen Compartments, vorliegen.

Diese Annahme wird in Satz 4.20 bewiesen. Zur Vereinfachung des Beweises wird zuvor das folgende Lemma gezeigt.

4.19 Lemma:

Sei $G \in \Gamma$ eine zulässige Teilnehmermenge eines Compartment Schemes. Der erweiterte Test auf Konsistenz werde nach Definition 4.10 durchgeführt und es gelte $E'^{0}_{M} = \{\}$.

Dann sind in den Ergebnismengen E_k jeweils genau t_j oder keine Teilnehmer eines Compartments C_j enthalten.

Beweis:
Nach Lemma 4.17 sind in einer Ergebnismenge E_k, wenn sie nichtleer ist, nur Teilnehmer eines Compartments enthalten.

Es ist also noch zu zeigen:
Wenn in einer Ergebnismenge ein Teilnehmer eines Compartments C_j enthalten ist, dann beträgt die Anzahl der Teilnehmer in E_k genau t_j.

Sei $\underline{M}$ nach Definition 4.7 die zu E_k gehörende Prüfstruktur. Ferner sei $G' := G \setminus X$ (mit $X \subseteq G$) diejenige Teilnehmermenge, für die $\underline{M}$ nach Lemma 4.9 die Minimalstruktur enthält.

Nach Lemma 4.18 muss für einen Teilnehmer P, der in E_k enthalten ist, gelten:

- $P \in C_j$ mit $|G' \cap C_j| = t_j$ und
- in G' tragen genau t Compartments zur Rekonstruktion bei.

Da die beiden obigen Voraussetzungen für alle Teilnehmer aus $G' \cap C_j$ gelten, folgt ebenfalls nach Lemma 4.18, dass alle Teilnehmer des Compartments $G' \cap C_j$ in E_k enthalten sind. Das sind genau t_j

4.20 Satz:

Sei $G \in \Gamma$ eine zulässige Teilnehmermenge eines Compartment Schemes. Der erweiterte Test auf Konsistenz werde nach Definition 4.10 durchgeführt. Der Test sei durchführbar (d.h. $E'^{0}_{M} = \{\}$).

Dann ist jede Vereinigungsmenge E^{k}_{C} leer oder sie enthält genau alle Teilnehmer eines Compartments, die in G vertreten sind.

Jedes Compartment C_j mit $|G \cap C_j| > t_j$ tritt in mindestens einer der Vereinigungsmengen auf.

Beweis:
Zu zeigen:

a) In den nichtleeren Vereinigungsmengen $E^{1}_{C}, \ldots, E^{g}_{C}$ sind *nur* Teilnehmer eines Compartments enthalten.

b) In den nichtleeren Vereinigungsmengen $E^{1}_{C}, \ldots, E^{g}_{C}$ sind *alle* in G vertretenen Teilnehmer eines Compartments enthalten.

c) Jedes Compartment C_j mit $|G \cap C_j| > t_j$ kommt in einer der Vereinigungsmengen $E^{1}_{C}, \ldots, E^{g}_{C}$ vor.

Zu a):
Nach Definition 4.10 werden die Vereinigungsmengen $E^{1}_{C}, \ldots, E^{g}_{C}$ durch Vereinigung der Ergebnismengen $E_1 \ldots E_g$ gebildet, deren Schnittmenge nichtleer ist.

Da nach Lemma 4.17 in den Ergebnismengen $E_1 \ldots E_g$ nur Teilnehmer enthalten sind, die zu demselben Compartment gehören, können in den Mengen $E^{1}_{C}, \ldots, E^{g}_{C}$ keine Teilnehmer unterschiedlicher Compartments enthalten sein.

Zu b):
Betrachtet werden alle t_j-elementigen Teilmengen T von $G \cap C_j$. Es wird zunächst gezeigt, dass jede dieser Teilmengen in einer der Ergebnismengen $E^{1}_{C}, \ldots, E^{g}_{C}$ auftritt.

Sei $P \in C_j$ mit $|G \cap C_j| \geq t_j$. Ferner sei M die Minimalstruktur von G. Dann kommt jede t_j-elementige Teilmenge T von $G \cap C_j$ in mindestens einer minimalen Menge von M vor.

Daraus folgt, dass für jede t_j-elementige Teilmenge T von $G \cap C_j$ mindestens eine Teilnehmermenge $G' := G \setminus X$ ($X \subseteq G$) existiert, für die gilt:

- $G' \cap C_j = T$, das heißt C_j ist minimal in G',
- die anderen an der Rekonstruktion beteiligten Compartments sind entweder nicht minimal in G' oder die Teilnehmer der Compartments sind nach Lemma 4.13 in einer der Ergebnismengen E'^{i}_{M} enthalten, und
- in G' nehmen genau t Compartments an der Rekonstruktion teil (t ist nach Definition 2.9 die Anzahl der für die Rekonstruktion benötigten Compartments).

Nach Lemma 4.18 und Definition 4.10 sind das genau die Voraussetzungen dafür, dass ein Teilnehmer $P \in T$ (und kein Teilnehmer $P' \notin T$) in allen minimalen Mengen der Teilnehmermenge G' enthalten ist. Das wiederum bedeutet nach Definition 4.10, dass jede t_j-elementige Untermenge T des Compartments C_j in mindestens einer der Ergebnismengen $E_1 \ldots E_g$ enthalten ist.

Da ferner nach Definition 2.9 $t_j \geq 2$ gilt, gibt es kein Untermengen T von C_j, die zu allen anderen Untermengen T' disjunkt sind. Insgesamt ist gewährleistet, dass durch Vereinigung der Ergebnismengen mit nichtleerer Schnittmenge zu den Mengen $E_C^1, \ldots, E_C^g$ alle Teilnehmer eines Compartments vereinigt werden.

Zu c):
Aus dem Argument zu b) folgt sofort, dass jedes Compartment C_j mit $|G \cap C_j| > t_j$ in mindestens einer der Mengen $E_C^1, \ldots, E_C^g$ enthalten ist.

Anmerkung:
Nach Satz 4.20 können dieselben Compartments auch in mehreren Vereinigungsmengen dargestellt werden.

In den Vereinigungsmengen liegen nach Satz 4.20 die Teilnehmer nach ihrer Zugehörigkeit zu Compartments sortiert vor. Der Weg dahin wird in der folgenden Abbildung noch einmal zusammengefasst.

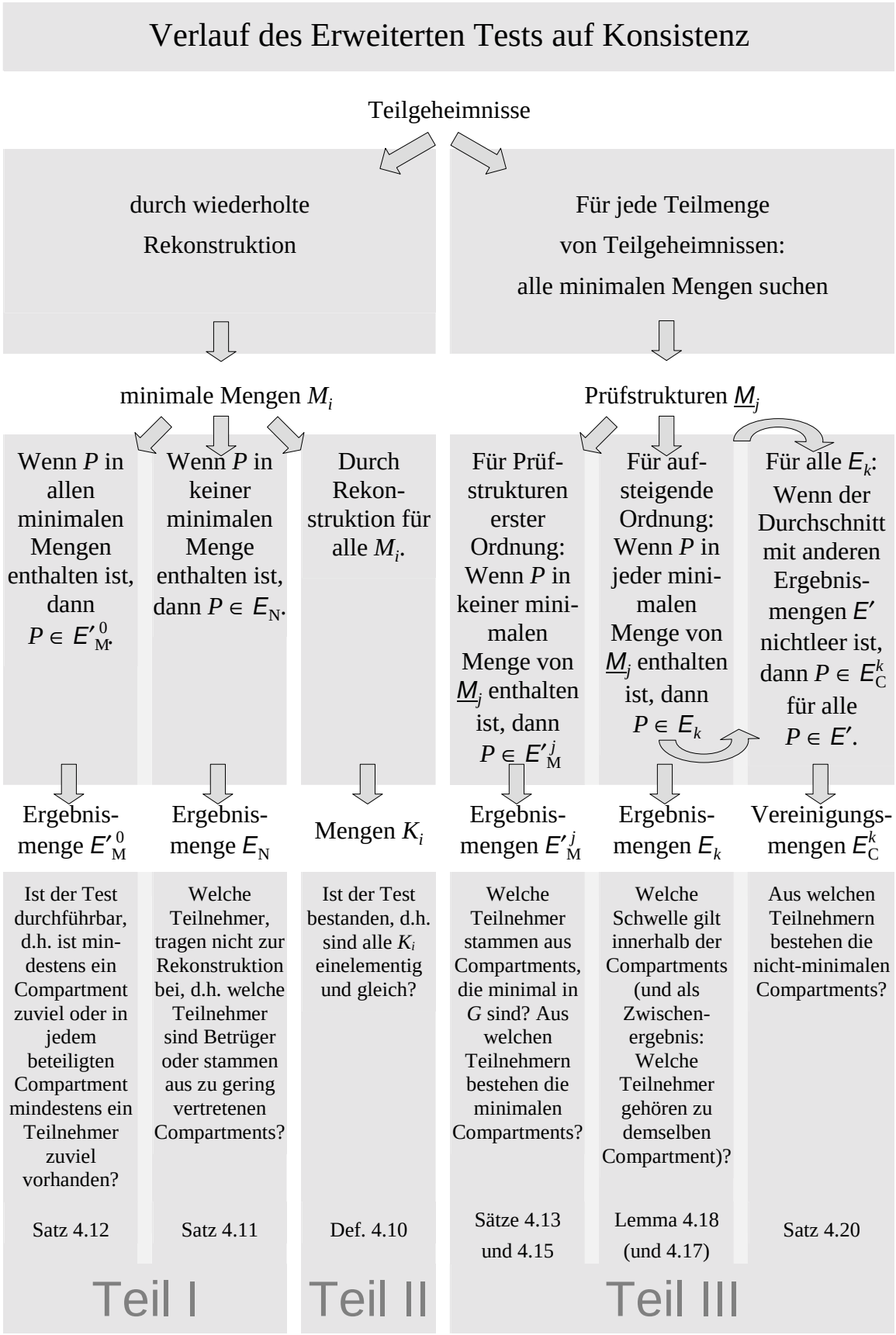


Abbildung 20: Verlauf des erweiterten Tests auf Konsistenz nach Definition 4.10

Teil I des Testes klärt, ob der Test durchführbar ist im Sinne der Überlegungen aus Kapitel 4.2.2. Ferner werden diejenigen Teilnehmer in der Menge E_N zusammengefasst, die nicht zur Rekonstruktion beitragen. Es handelt sich dabei entweder um Teilnehmer aus zu gering vertretenen Compartments oder um Betrüger.

Teil II des erweiterten Testes besteht in der Prüfung, ob die Rekonstruktionen der verschiedenen minimalen Mengen dasselbe Ergebnis liefern. Wenn die Ergebnisse nicht konsistent sind, liegt auf jeden Fall ein Betrug vor.

In dem Teil III des Tests werden zunächst die Teilnehmer ermittelt, die aus minimalen Compartments (Definition 2.10) stammen. Diese Teilnehmer können den Compartments, aus denen sie stammen, zugeordnet werden, wenn $E'^{0}_{M} = \{\}$ gilt. Für diese minimalen Compartments kann die Konsistenz nur im Vergleich zu den anderen Compartments überprüft werden. Eine Konsistenzaussage für die einzelnen Teilnehmer innerhalb der minimalen Compartments kann nicht getroffen werden.

Schließlich werden die restlichen Teilnehmer in den Vereinigungsmengen $E^1_C, \ldots, E^g_C$ nach ihrer Zugehörigkeit zu den Compartments sortiert. Die Schwelle eines Compartments ergibt sich aus der Mächtigkeit der Ergebnismengen $E_1 \ldots E_g$.

Durch die Ergebnisse des Teil III des erweiterten Tests auf Konsistenz können dann Aussagen darüber getroffen werden, wie gering die Wahrscheinlichkeit ist, dass ein Betrug stattgefunden hat, bzw. wie sicher das Ergebnis der Rekonstruktion ist. Diese Sicherheitsaussagen werden in Abschnitt 4.2.4 abgeleitet.

Für die Beweise der obigen Sätze und Lemmas wurden keine Eigenschaften der geometrischen Compartment Schemes benötigt. Die gezeigten Eigenschaften des erweiterten Tests auf Konsistenz nach Definition 4.10 gelten folglich unabhängig von der Realisierung.

4.2.4 Sicherheitsaussagen für den erweiterten Test auf Konsistenz in der geometrischen Realisierung

Der erweiterte Test auf Konsistenz ist in der Lage, die Teilnehmer nach ihrer Zugehörigkeit zu den Compartments zu sortieren. Es bleibt die Frage zu klären, mit welcher Wahrscheinlichkeit eine Zugriffskontrollinstanz einen Betrug oder einen Betrüger mit Hilfe des Testes entdecken kann.

Diese Frage kann nur dann beantwortet werden, wenn eine konkrete Realisierung betrachtet wird. Die allgemeine Definition für Secret Sharing Schemes (2.3) macht lediglich Aussagen darüber, wie sich ein System gegenüber berechtigten und unberechtigten Teilnehmerkonstellationen verhält, wenn alle Teilnehmer ihr tatsächliches Geheimnis angeben. Die Möglichkeit, dass Teilnehmer nicht das ihnen zugeteilte Teilgeheimnis angeben, kommt in der Definition nicht vor. Sie kann daher nur in einer konkreten Realisierung betrachtet werden. Für die folgenden Sicherheitsaussagen wird ein geometrisches Compartment Scheme nach Definition 4.1 vorausgesetzt.

4.2.4.1 Prüfbare Teilnehmermengen

Die Sätze der folgenden Abschnitte haben eine gemeinsame Voraussetzung. Diese Voraussetzung wird in Definition 4.21 formuliert.

4.21 Definition: PRÜFBARE TEILNEHMERMENGEN EINES COMPARTMENT SCHEMES

Sei $G \in \Gamma$ eine zulässige Teilnehmermenge eines Compartment Schemes nach Definition 2.9. Ferner sei x_i die Anzahl der Betrüger, die im Compartment C_i an der Rekonstruktion teilnehmen. G heißt *prüfbare Teilnehmermenge*, wenn für höchstens t - 1 Compartments gilt:

$$x_i \geq t_i$$

Anmerkung:
Wenn in einem Compartment $x_i < t_i$ gilt, dann trägt innerhalb dieses Compartments mindestens ein ehrlicher Teilnehmer zur Rekonstruktion bei. Wenn diese Voraussetzung höchstens für $t - 1$ Compartment verletzt wird, dann ist mindestens ein Compartment mit mindestens einem ehrlichen Teilnehmer an der Rekonstruktion beteiligt. Folglich ist bei prüfbaren Teilnehmermengen gewährleistet, dass mindestens ein ehrlicher Teilnehmer zur Rekonstruktion beiträgt.

4.2.4.2 Integrität des rekonstruierten Ergebnisses

Zunächst wird die Frage untersucht, wie hoch die Wahrscheinlichkeit dafür ist, dass die Teilnehmer tatsächlich K_0 und nicht einen anderen Schnittpunkt $K_x \neq K_0$ mit der Geheimnisgeraden rekonstruieren, wenn der Test auf Konsistenz bestanden wurde.

4.22 Satz:

Sei $G \in \Gamma$ eine nach Definition 4.21 prüfbare Teilnehmermenge eines geometrisch realisierten Compartment Schemes, K_0 sei das verschlüsselte Geheimnis. Der erweiterte Test auf Konsistenz werde nach Definition 4.10 durchgeführt. Der Test sei durchführbar und werde bestanden.

Dann ist das rekonstruierte Geheimnis K_x mit der Wahrscheinlichkeit

$$p \geq p_E(t_1 + t_2 + \ldots + t_{t+1})$$

gleich K_0. p_E ist die in Definition 3.15 eingeführte Erfolgswahrscheinlichkeit des erweiterten Tests auf Konsistenz.

Beweis:
Der Test ist nach Voraussetzung durchführbar und wird bestanden. Daraus folgt mit Definition 4.10: $E_M^0 = \{\}$. Nach Satz 4.12 muss daher eine der beiden folgenden Voraussetzungen erfüllt sein.

i) In jedem beteiligten Compartment nimmt mindestens ein Teilnehmer mehr an der Rekonstruktion teil, als benötigt wird.
ii) An der Rekonstruktion ist mindestens ein Compartment mehr beteiligt, als erforderlich.

Zu i):
Wenn das rekonstruierte Geheimnis durch Anwesenheit von Betrügern verfälscht, der Test auf Konsistenz jedoch bestanden werden soll, dann muss in mindestens einem beteiligten Compartment gelten: Die mindestens t_i+1 Teilnehmer des Compartments C_i enthalten Betrüger und spannen dennoch einen maximal (t_i-1)- dimensionalen Raum auf. Die Wahrscheinlichkeit p_i für diesen erfolgreichen Betrug ist nach Satz 3.14 (mit p_B aus Definition 3.15):

$$p_i \leq p_B(t_i)$$

Zu ii):
Der für die gesuchte Wahrscheinlichkeit ungünstigste Fall ist die Beteiligung von genau einem Compartment mehr, als zur Rekonstruktion erforderlich ist. Die beteiligten Compartments seien $C_1, C_2, \ldots, C_{t+1}$. Die Anzahl der Teilnehmer in diesen Compartments sei (im ebenfalls ungünstigsten Fall) $t_1, t_2, \ldots, t_{t+1}$. Aus dem Bestehen des Testes auf Konsistenz folgt, dass jeweils t dieser t+1 Compartments das Geheimnis K_x rekonstruieren können.

Zunächst werden die Teilnehmer der Compartments $C_1, \ldots, C_t$ betrachtet. Sie erzeugen einen maximal (t_1+…+t_t-1)-dimensionalen Raum durch K_x. Ferner legen diese Teilnehmer nach Definition 4.1 einen (t-1)-dimensionalen Unterraum B_0 durch K_x fest. Das Erzeugnis der Teilnehmer des Compartments C_{t+1} muss mit B_0 einen gemeinsamen Punkt haben (da t beliebige Compartments K_x rekonstruieren können). Daraus folgt, dass die mindestens $t_1 + t_2 + \ldots + t_{t+1}$ Teilnehmer der beteiligten Compartments einen maximal (t_1+…+t_{t+1}-2)–dimensionalen Raum erzeugen. Die Wahrscheinlichkeit p' für diese Situation ist bei Anwesenheit von Betrügern nach Satz 3.14:

$$p' \leq p_B(t_1 + t_2 + \ldots + t_{t+1})$$

Insgesamt gilt für die Erfolgswahrscheinlichkeit p des Testes, da p_B mit t wächst.

$$p \geq 1 - p' = p_E(t_1 + t_2 + \ldots + t_{t+1})$$

4.2.4.3 Anwesenheit von Betrügern bei dem Test

Der nächste Satz gibt die Wahrscheinlichkeit dafür an, dass ein Betrüger bei Durchführung des erweiterten Tests auf Konsistenz nach Definition 4.10 in der Ergebnismenge E_N enthalten ist. Nach Satz 4.11 sind in E_N genau diejenigen Teilnehmer enthalten, die nicht zur Rekonstruktion beitragen. Gesucht ist also die Wahrscheinlichkeit, dass ein Betrüger nicht zur Rekonstruktion beiträgt (und sie daher nicht beeinflusst).

4.23 Satz:

Sei $G \in \Gamma$ eine nach Definition 4.21 prüfbare Teilnehmermenge eines geometrisch realisierten Compartment Schemes. Der erweiterte Test auf Konsistenz werde nach Definition 4.10 durchgeführt. Der Test sei durchführbar (d.h. $E_M^0 = \{\}$).

Dann ist ein Betrüger mit der Wahrscheinlichkeit

$$p \geq 1 - \frac{q^{d-1} + q^{d-2} + \ldots + q - 1}{q^d + q^{d-1} + \ldots + q^2 - 1}$$

in der Menge E_N enthalten.

Beweis:
Ein Betrüger ist nach Definition 4.10 genau dann in E_N enthalten, wenn er nicht im Erzeugnis der ehrlichen, an der Rekonstruktion beteiligten Teilnehmer liegt.

Nach Definition 3.1 wird ein geometrisches Secret Sharing Scheme in PG(d, q), einem projektiven Raum der Dimension d realisiert. Für Compartment Schemes gilt nach Definition 4.1 $d = (t_1\text{-}1) + (t_2\text{-}1) + \ldots + (t_r\text{-}1) + (t\text{-}1) + s$. Ferner gilt nach Definition 4.1 für die Dimension d' des Erzeugnisses der ehrlichen Teilnehmer:

$$d' \leq d^* = \dim B_0^* = d - 1.$$

Folglich liegen in dem Erzeugnis der ehrlichen Teilnehmer höchstens (für $d' = d^*$ und s = 1) $q^{d-1} + q^{d-2} + \ldots + q + 1$ Punkte, von denen der Schnittpunkt des Erzeugnisses mit der Geheimnisgeraden sowie das Teilgeheimnis des Betrügers (als mögliche Teilgeheimnisse) abgezogen werden.

Ein Betrüger hat a priori alle Punkte aus PG(d, q) zur Auswahl. Sein eigener und die Punkte der Geheimnisgeraden kommen für die Auswahl nicht in Frage, es bleiben also $q^d + q^{d-1} + \ldots + q^2 - 1$ Punkte.

Demnach gilt für die Wahrscheinlichkeit, dass ein Betrüger, der zufällig einen Punkt aus PG(d, q) wählt, in E_N enthalten ist:

$$p \geq 1 - \frac{q^{d-1} + q^{d-2} + \ldots + q - 1}{q^d + q^{d-1} + \ldots + q^2 - 1}$$

Der Satz lässt folgenden wichtigen Schluss zu:
Wenn $E_N = \{\}$, dann sind mit der angegebenen Wahrscheinlichkeit p alle Teilnehmer ehrlich.

Die andere Richtung der Aussage, nämlich von $E_N \neq \{\}$ auf das Vorhandensein eines oder mehrerer Betrüger zu schließen, ist im allgemeinen nicht richtig. In E_N sind nach Satz 4.11 auch diejenigen *ehrlichen* Teilnehmer enthalten, die nicht zur Rekonstruktion

beitragen, weil sie aus Compartments stammen, die in der betrachteten Teilnehmermenge nicht mit hinreichend vielen Teilnehmern vertreten sind.

4.2.4.4 Sicherheitsaussagen für die gefundenen Compartments

Durch den erweiterten Test auf Konsistenz werden die Teilnehmer, die an der Rekonstruktion beteiligt sind, nach ihrer Zugehörigkeit zu den Compartments sortiert. In Abschnitt 4.2.4.3 wurde bereits die Wahrscheinlichkeit dafür ermittelt, dass ein Betrüger in der Menge E_N enthalten ist. Im folgenden wird noch die Frage beantwortet, wie hoch die Wahrscheinlichkeit dafür ist, dass in einem an der Rekonstruktion beteiligten Compartment kein Betrüger enthalten ist.

4.24 Satz:

Sei $G \in \Gamma$ eine nach Definition 4.21 prüfbare Teilnehmermenge eines geometrisch nach Definition 4.1 in PG(d, q) realisierten Compartment Schemes. Der erweiterte Test auf Konsistenz werde nach Definition 4.10 durchgeführt. Der Test sei durchführbar (d.h. $E_M^0 = \{\}$).

Ferner gelte für das Compartment C_i:

$$|C_i \cap G| = t_i + v \text{ mit } v \geq 1.$$

Dann ist mit der Wahrscheinlichkeit

$$p \geq 1 - \binom{|G|}{t_i + v} \left(\frac{q^{t_i-1} + q^{t_i-2} + \ldots + q}{q^d + q^{d-1} + \ldots + q^t - q} \right)^v$$

kein Betrüger in C_i enthalten.

Beweis:
Aus $|C_i \cap G| = t_i + v$ folgt nach Definition 4.1, dass $t_i + v$ Punkte in einem (t_i-1)-dimensionalen Raum liegen, der genau einen Schnittpunkt mit B_0 hat. Gesucht wird zunächst die Wahrscheinlichkeit dafür, dass unter diesen ($t_i + v$) Teilnehmern Betrüger sind.

Der Beweis erfolgt analog zu dem Beweis zu Satz 3.14. Der wesentliche Unterschied besteht lediglich darin, dass dort für *alle* Untermengen der Teilnehmermenge G die Wahrscheinlichkeit ermittelt dafür wurde, dass sie die obige Bedingung (für $v = 1$) erfüllen. Anschließend wurden die Wahrscheinlichkeiten addiert. Im Gegensatz dazu müssen hier nur die Untermengen von G betrachtet werden, welche die Mächtigkeit $t_i + v$ besitzen.

Die Anzahl der ($t_i + v$)-elementigen Untermengen von G ist

$$n := \binom{|G|}{t_i + v}.$$

Seien $X_1, X_2, X_3, \ldots, X_{t_i+v}$ die Teilgeheimnispunkte der $t_i + v$ Teilnehmer. Sie müssen in einem (t_i-1)-dimensionalen Raum durch B_0 liegen. Die Punkte $X_1, X_2, X_3, \ldots, X_{t_i}$ mögen

einen (t_i-1)-dimensionalen Raum durch $B \in B_0$ (mit $B \neq B_0 \cap K$) erzeugen. Im folgenden wird die Wahrscheinlichkeit p^* dafür ermittelt, dass die Punkte X_{t_i+1}, …, X_{t_i+v} in diesem Raum liegen.

In dem erzeugten (t_i-1)-dimensionalen Raum liegen $q^{t_i-1} + q^{t_i-2} + \ldots + q + 1$ Punkte, von denen der Schnittpunkt mit B_0 abgezogen wird, da die Punkte X_{t_i+1}, …, X_{t_i+v} nicht in B_0 liegen dürfe.

In PG(d, q) gibt es insgesamt $q^d + q^{d-1} + \ldots + q + 1$ Punkte, von denen die (q - 1) Punkte der Geheimnisgeraden und die Punkte von B_0 a priori ausgeschlossen werden können. In B_0 liegen $q^{t-1} + q^{t-2} + \ldots + q + 1$ Punkte (da nach Definition 4.1 gilt: dim $B_0 = t - 1$, t ist die Anzahl der für die Rekonstruktion erforderlichen Compartments). Insgesamt stehen also

$$(q^d + q^{d-1} + \ldots + q + 1) - (q^{t-1} + q^{t-2} + \ldots + q + 1) - q$$

Punkte zur Auswahl (wenn beachtet wird, dass B_0 und die Geheimnisgerade einen Punkt gemeinsam haben).

Für die Wahrscheinlichkeit p^* gilt also:

$$p^* \leq \left(\frac{q^{t_i-1} + q^{t_i-2} + \ldots + q}{q^d + q^{d-1} + \ldots + q^t - q} \right)^v$$

Für die Wahrscheinlichkeit p' eines erfolgreichen Betruges gilt:

$$p' \leq n p^*$$

und insgesamt folgt

$$p \geq 1 - p' = 1 - n p^* = 1 - \binom{|G|}{t_i + v} p^*$$

Anmerkung:
Je mehr Teilnehmer innerhalb eines Compartments an der Rekonstruktion teilnehmen (d.h. je größer v ist), desto geringer die Wahrscheinlichkeit, dass ein Betrüger unter den Teilnehmern ist.

Nach Satz 4.24 gilt für die Wahrscheinlichkeit eines erfolgreichen Betruges:

$$p' \leq \binom{|G|}{t_i + v} \left(\frac{q^{t_i-1} + q^{t_i-2} + \ldots + q}{q^d + q^{d-1} + \ldots + q^t - q} \right)^v$$

Nach Definition 4.1 gilt für die Dimension d des projektiven Raumes, in dem ein Compartment Scheme realisiert wird:

$$d := (t_1\text{-}1) + (t_2\text{-}1) + \ldots + (t_r\text{-}1) + (t\text{-}1) + s$$

Daraus folgt die Abschätzung $d \geq (t_i\text{-}1) + (t\text{-}1) + s$ für $i = 1, \ldots, r$ (wobei das Gleichheitszeichen für $r = 1$ gilt). Daraus wiederum folgt:

$$\lim_{q \to \infty} p' = 0 \text{ (für } v \geq 1).$$

Die mit den letzten Sätzen abgeleiteten Aussagen des Testes sind in der nächsten Abbildung zusammengefasst. Sie gelten jeweils mit vorgebbarer Wahrscheinlichkeit.

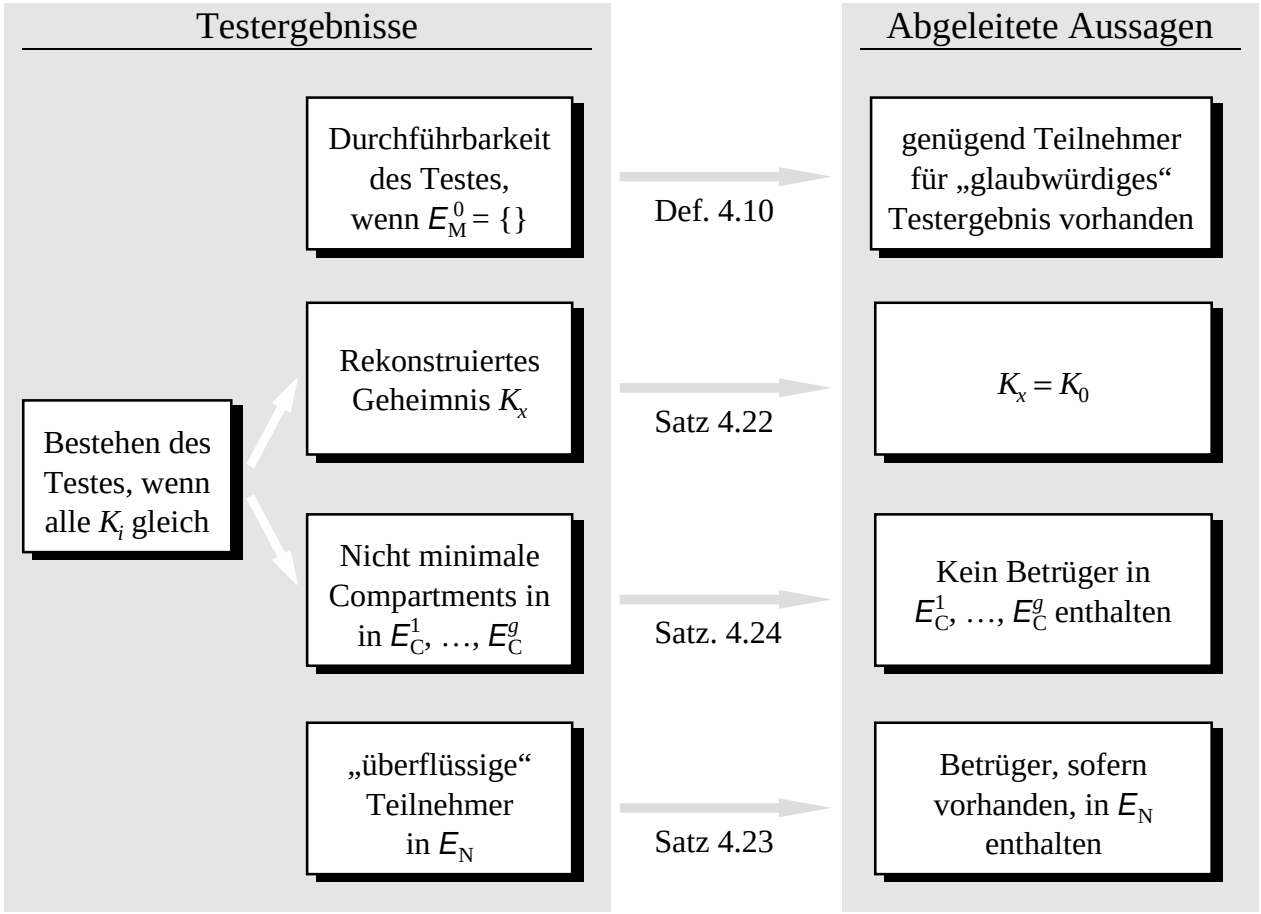


Abbildung 21: Aussagen des erweiterten Tests auf Konsistenz

4.3 Beispiel

Im folgenden wird der erweiterte Test auf Konsistenz für Compartment Schemes an einem Beispiel durchgeführt. Ein (2; 2, 2, 2)-Compartment Scheme sei geometrisch realisiert. Die Teilnehmer $P_1, P_2, \ldots, P_9$ seien ehrlich, P_{10} und P_{11} seien Betrüger. Ihre Teilgeheimnispunkte liegen mit den Punkten von P_6 und P_8 in einer Ebene. Die Situation ist in der Abbildung dargestellt.

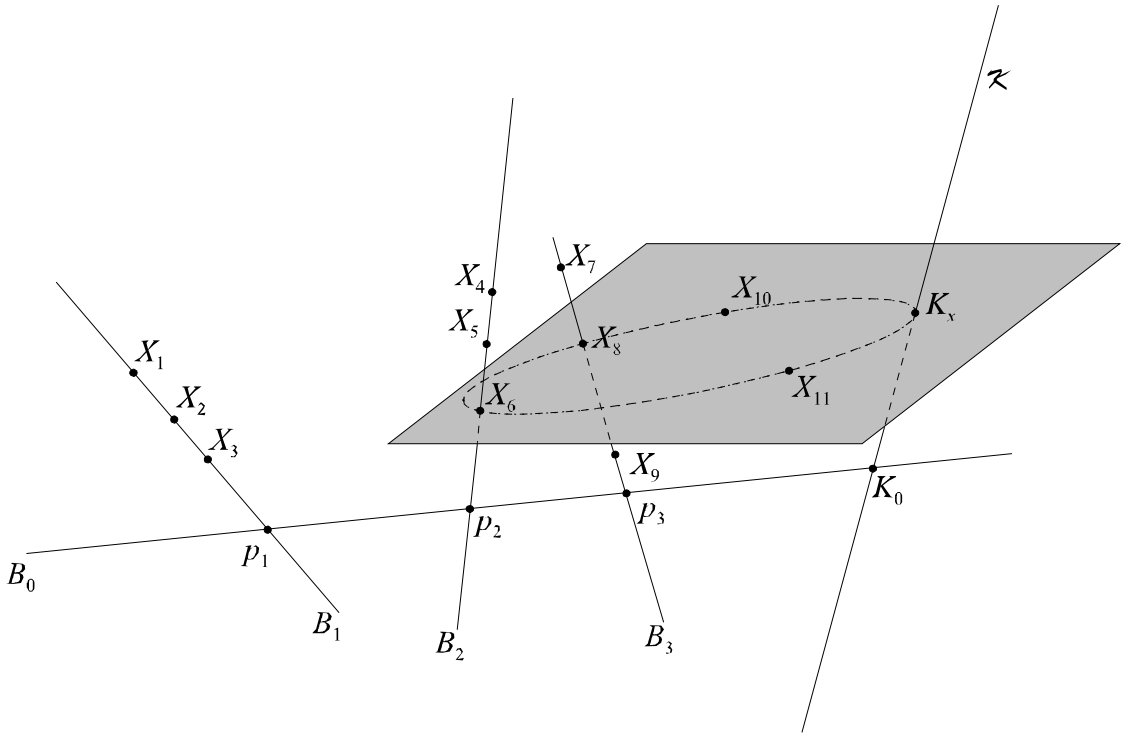


Abbildung 22: Ein (2; 2, 2, 2)-Compartment Scheme mit zwei Betrügern

In den nächsten Abschnitten wird für verschiedene Teilnehmermengen der Verlauf des erweiterten Testes auf Konsistenz beschrieben.

4.3.1 Test wird bestanden

Gegeben sei die Teilnehmermenge

$$G = \{P_1, P_2, P_3, P_4, P_5, P_6, P_{10}\}.$$

Die folgende Tabelle enthält die neun minimalen Mengen von *G*. Analog zu der Tabelle in Abschnitt 4.2.3 auf Seite 64 sind in den Spalten- bzw. Zeilenköpfen jeweils die Teilnehmer eingetragen, die in jeder minimalen Menge einer Spalte bzw. Zeile enthalten sind.

	P_4, P_5	P_4, P_6	P_5, P_6
P_1, P_2	$M_1 = \{P_1, P_2, P_4, P_5\}$	$M_4 = \{P_1, P_2, P_4, P_6\}$	$M_7 = \{P_1, P_2, P_5, P_6\}$
P_1, P_3	$M_2 = \{P_1, P_3, P_4, P_5\}$	$M_5 = \{P_1, P_3, P_4, P_6\}$	$M_8 = \{P_1, P_3, P_5, P_6\}$
P_2, P_3	$M_3 = \{P_2, P_3, P_4, P_5\}$	$M_6 = \{P_2, P_3, P_4, P_6\}$	$M_9 = \{P_2, P_3, P_5, P_6\}$

Für die in Teil I des Tests berechneten Mengen gilt:

$$E'^{0}_{\mathrm{M}} := \{ P \in G \mid P \in M_i \text{ für } \textit{alle } i = 1, 2, \ldots, m\} = \{\}$$
$$E_{\mathrm{N}} := \{ P \in G \mid P \notin M_i \text{ für } \textit{alle } i = 1, 2, \ldots, m\} = \{P_{10}\}$$

Der Test ist demnach durchführbar ($E'^{0}_{\mathrm{M}} = \{\}$), über die Ehrlichkeit des Teilnehmers P_{10} kann keine Aussage gemacht werden ($E_{\mathrm{N}} = \{P_{10}\}$).

In Teil II des Tests wird für alle minimalen Mengen die Rekonstruktion durchgeführt. Sei K_i das Rekonstruktionsergebnis der minimalen Menge M_i, dann gilt:

$$K_1 = K_2 = K_3 = K_4 = K_5 = K_6 = K_7 = K_8 = K_9 \; (= K_0)$$

Der Test wird bestanden.

In Teil III, Schritt 1 des Test ergibt sich nach den Definitionen 4.10 und 4.7:

$$E'^{i}_{\mathrm{M}} = \{\} \quad \text{für } i = 1, 2, \ldots, |G|$$

An der Rekonstruktion sind daher nach den Sätzen 4.13 und 4.15 keine minimalen Compartments beteiligt.

Die folgende Tabelle gibt die Ergebnisse des Schrittes 2 des Teils III des Test wieder. Die Spalte 2 der Tabelle enthält alle einelementigen Teilmengen G_i der Teilnehmermenge G. Nach Definition 4.7 werden für diese Mengen G_i jeweils die Prüfstrukturen $\underline{M_i}$ gebildet ($\underline{M_i}$ enthält alle minimalen Mengen, deren Durchschnitt mit G_i leer ist). E_i enthält nach Definition 4.10 jeden Teilnehmer, der in allen minimalen Mengen der Prüfmenge $\underline{M_i}$ vorkommt. Daraus werden schließlich die Mengen E^{i}_{C} gebildet, welche die Teilnehmer nach ihrer Zugehörigkeit zu den Compartments sortieren:

i	G_i	$\underline{M_i}$	E_i	E^{i}_{C}
1	P_1	M_3, M_6, M_9	P_2, P_3	P_1, P_2, P_3
2	P_2	M_2, M_5, M_8	P_1, P_3	P_1, P_2, P_3
3	P_3	M_1, M_4, M_7	P_1, P_2	P_1, P_2, P_3
4	P_4	M_7, M_8, M_9	P_5, P_6	P_4, P_5, P_6
5	P_5	M_4, M_5, M_6	P_4, P_6	P_4, P_5, P_6
6	P_6	M_1, M_2, M_3	P_4, P_5	P_4, P_5, P_6
7	P_{10}	$M_1, M_2, M_3, M_4, M_5, M_6, M_7, M_8, M_9$	---	---

Die beiden beteiligten Compartments werden korrekt rekonstruiert. Teilnehmer P_{10} bleibt zwar als Betrüger unerkannt, das Rekonstruktionsergebnis wird jedoch durch ihn nicht verfälscht.

4.3.2 Test wird nicht bestanden

Gegeben sei die Teilnehmermenge

$$G = \{P_1, P_2, P_4, P_5, P_8, P_{10}, P_{11}\}.$$

Zu dieser Teilnehmermenge existieren zwei minimalen Mengen:

$$M_1 = \{P_1, P_2, P_4, P_5\}$$
$$M_2 = \{P_8, P_{10}, P_{11}\}$$

Für die in Teil I des Tests berechneten Mengen gilt:

$$E'^0_M := \{ P \in G \mid P \in M_i \text{ für } \textit{alle } i = 1, 2, \ldots, m\} = \{\}$$
$$E_N := \{ P \in G \mid P \notin M_i \text{ für } \textit{alle } i = 1, 2, \ldots, m\} = \{\}$$

Der Test ist also nach Definition 4.10 durchführbar, da $E'^0_M = \{\}$.

In Teil II des Testes ergeben sich für die beiden minimalen Mengen unterschiedliche Geheimnisse, der Test wird nicht bestanden:

$$K_0 = K_1 \neq K_2 = K_x$$

Die Betrüger sind in dieser Konstellation nicht in der Ergebnismenge E_N enthalten, da sie in einer Ebene mit einem Punkt der Geheimnisgeraden und einem ehrlichen Teilnehmer liegen. Der Test wird jedoch aufgrund der Gegenwart von Betrügern nicht bestanden.

4.3.3 Test ist nicht durchführbar

Gegeben sei die Teilnehmermenge

$$G = \{P_1, P_2, P_3, P_4, P_5\}.$$

Zu dieser Teilnehmermenge existieren drei minimalen Mengen:

$$M_1 = \{P_1, P_2, P_4, P_5\}$$
$$M_2 = \{P_1, P_3, P_4, P_5\}$$
$$M_3 = \{P_2, P_3, P_4, P_5\}$$

Für die in Teil I des Tests berechneten Mengen gilt:

$$E'^0_M := \{ P \in G \mid P \in M_i \text{ für } \textit{alle } i = 1, 2, \ldots, m\} = \{P_4, P_5\}$$
$$E_N := \{ P \in G \mid P \notin M_i \text{ für } \textit{alle } i = 1, 2, \ldots, m\} = \{\}$$

Der Test ist also nach Definition 4.10 nicht durchführbar, da

- die beiden beteiligten Compartments für die Rekonstruktion erforderlich sind und
- die Teilnehmer P_4 und P_5 aus einem in G minimal vertretenen Compartment stammen.

4.3.4 Test rekonstruiert falsches Ergebnis

Gegeben sei die Teilnehmermenge

$$G = \{P_6, P_8, P_{10}, P_{11}\}.$$

Zu dieser Teilnehmermenge existieren vier minimalen Mengen:

$$M_1 = \{P_6, P_8, P_{10}\}$$
$$M_2 = \{P_6, P_8, P_{11}\}$$
$$M_3 = \{P_6, P_{10}, P_{11}\}$$
$$M_4 = \{P_8, P_{10}, P_{11}\}$$

Für die in Teil I des Tests berechneten Mengen gilt:

$$E'^{0}_{\mathrm{M}} := \{ P \in G \mid P \in M_i \text{ für } \textit{alle } i = 1, 2, \ldots, m\} = \{\}$$
$$E_{\mathrm{N}} := \{ P \in G \mid P \notin M_i \text{ für } \textit{alle } i = 1, 2, \ldots, m\} = \{\}$$

Der Test ist nach Definition 4.10 durchführbar, da $E'^{0}_{\mathrm{M}} = \{\}$.

Für alle minimalen Mengen wird dasselbe Geheimnis rekonstruiert. Es gilt

$$K_1 = K_2 = K_3 = K_4 \ (= K_x)$$

Der Test wird also trotz der Gegenwart von Betrügern bestanden. Die ehrlichen Teilnehmer P_6 und P_8 würden dem falschen Geheimnis K_x trauen.

In Teil III des Testes werden die vier Teilnehmer demselben Compartment zugeordnet:

i	G_i	M_i	E_i	E^i_{C}
1	P_6	M_4	P_8, P_{10}, P_{11}	P_6, P_8, P_{10}, P_{11}
2	P_8	M_3	P_6, P_{10}, P_{11}	P_6, P_8, P_{10}, P_{11}
3	P_{10}	M_2	P_6, P_8, P_{11}	P_6, P_8, P_{10}, P_{11}
4	P_{11}	M_1	P_6, P_8, P_{10}	P_6, P_8, P_{10}, P_{11}

4.4 Threshold Schemes als Spezialfall

Der erweiterte Test auf Konsistenz, wie er mit Definition 4.10 eingeführt wurde ist gleichermaßen auf die Threshold Schemes anwendbar. Im folgenden wird gezeigt, dass es sich bei dem in Definition 3.12 eingeführten Test für Threshold Schemes um einen Spezialfall des hier behandelten Tests handelt.

Bevor die Entsprechungen im einzelnen dargelegt werden, sei noch darauf hingewiesen, dass ein Compartment Scheme mit $t = 1$ nicht in jedem Fall ein Threshold Scheme darstellt. $t = 1$ bedeutet, dass nur ein Compartment für die Rekonstruktion des Geheimnisses erforderlich ist. Dennoch könnten die Teilnehmer unterschiedlichen Compartments zugeteilt sein und innerhalb der Compartments könnten unterschiedliche Schwellen gelten. Insbesondere könnte dann ein Teilnehmer aus dem Compartment C_i

einen Teilnehmer aus C_j für $i \neq j$ nicht vertreten. Dieser Sachverhalt kann bei einem Threshold Scheme nicht auftreten.

Ein Threshold Scheme ist ein Compartment Scheme nach Definition 2.9 mit $t = 1$ und $r = 1$.

4.25 Satz:

Sei $G \in \Gamma$ eine zulässige Teilnehmermenge eines geometrisch nach Definition 3.2 in PG(d, q) realisierten Threshold Schemes. Die Tests auf Konsistenz werden nach den Definitionen 3.12 und 4.10 durchgeführt.

Dann gilt mit der Wahrscheinlichkeit $p_E(t)$:

$$D \neq \{\} \quad \Leftrightarrow \quad E'^0_M = \{\}$$

Beweis:
Zu zeigen:
a) $D \neq \{\} \quad \Rightarrow \quad E'^0_M = \{\}$
b) $E'^0_M = \{\} \quad \Rightarrow \quad D \neq \{\}$

Zu a):
Nach Definition 3.12 gilt:

$$D = \left\{ K \in K \middle| K \in K_i, K_j \ (i \neq j) \right\}$$

D enthält demnach alle Elemente der Geheimnismenge K, die von mindestens zwei minimalen Mengen von G rekonstruiert werden. Nach Satz 3.14 folgt daraus mit der Wahrscheinlichkeit $p_E(t)$, dass mindestens $t + 1$ ehrliche Teilnehmer in G enthalten sind. Daraus wiederum folgt, dass keiner der Teilnehmer in jeder minimalen Menge von G enthalten ist und somit gilt nach Definition 4.10:

$$E'^0_M = \{\}$$

Zu b):
Nach Definition 4.10 gilt:

$$E'^0_M := \{ P \in G \mid P \in M_i \text{ für } \textit{alle } i = 1, 2, \ldots, m)\}$$

E'^0_M enthält demnach alle Teilnehmer, die in jeder minimalen Menge von G enthalten sind. Nach Satz 4.12 folgt aus $E'^0_M = \{\}$, dass in G

- ein Compartment oder
- in jedem Compartment ein Teilnehmer

mehr enthalten ist, als zur Rekonstruktion erforderlich ist.

Für ein Threshold Scheme kann die erste Bedingung nicht erfüllt sein, folglich muss die zweite Bedingung erfüllt sein. Daraus folgt, dass mindestens $t + 1$ Teilnehmer in G enthalten sind, die mit mindestens der Wahrscheinlichkeit $p_E(t)$ ehrlich sind.

Daraus folgt nach Definition 3.12:

$$D \neq \{\}$$

Der obige Satz besagt, dass beide Tests unter denselben Voraussetzungen durchführbar sind.

4.26 Satz:

Sei $G \in \Gamma$ eine zulässige Teilnehmermenge eines geometrisch nach Definition 3.2 in PG(d, q) realisierten Threshold Schemes. Die Tests auf Konsistenz werden nach den Definitionen 3.12 und 4.10 durchgeführt.

Dann wird der Test auf Konsistenz nach Definition 3.12 genau dann bestanden, wenn auch der Test auf Konsistenz nach Definition 4.10 bestanden wird.

Beweis:
Die Aussage des Satzes folgt sofort aus den in Bezug auf das Bestehen des Testes identischen Definitionen 3.12 und 4.10.

4.27 Satz:

Sei $G \in \Gamma$ eine zulässige Teilnehmermenge eines geometrisch nach Definition 3.2 in PG(d, q) realisierten Threshold Schemes. Die Tests auf Konsistenz werden nach den Definitionen 3.12 und 4.10 durchgeführt. Die Tests seien durchführbar, d.h. es gelte $D \neq \{\}$ bzw. $E'^{0}_{M} = \{\}$.

Dann gilt für die nach Definition 3.12 berechnete Menge E_B und die nach Definition 4.10 ermittelte Menge E_N mit der Wahrscheinlichkeit $p_E(t)$:

$$E_B = E_N$$

Beweis:
Zu zeigen:
a) $P \in E_B \Rightarrow P \in E_N$
b) $P \in E_N \Rightarrow P \in E_B$

Zu a):
Nach Satz 3.16 sind in E_B mit der Wahrscheinlichkeit $p_E(t)$ genau alle Betrüger im Sinne von Definition 2.13 enthalten. Das bedeutet für geometrische Threshold Schemes nach Definition 3.2, dass in E_B alle Teilnehmer enthalten sind, deren Teilgeheimnisse nicht im Indikatorblock B_0 liegen.

Ein Teilnehmer P, dessen Teilgeheimnis nicht in B_0 liegt, trägt nicht zur Rekonstruktion bei und ist daher in keiner minimalen Menge enthalten. Daher gilt nach Definition 4.10:

$$P \in E_N$$

Zu b):
Aus $P \in E_N$ folgt, dass P in keiner minimalen Menge enthalten ist. Daraus folgt nach Definition 3.12 für den Test auf Konsistenz für Threshold Schemes: $P \notin E_E$, denn

$$E_E := \{ P \in G \mid \text{es existiert ein } i \text{ mit } P \in M_i \text{ und } K_i \in D\} \text{ und } P \notin M_i \text{ für alle } i.$$

Da nach Definition 3.12 ferner $E_B := G \setminus E_E$ gilt, folgt

$$P \in E_B.$$

4.28 Satz:

Sei $G \in \Gamma$ eine zulässige Teilnehmermenge eines geometrisch nach Definition 3.2 in PG(d, q) realisierten Threshold Schemes. Die Tests auf Konsistenz werden nach den Definitionen 3.12 und 4.10 durchgeführt. Die Tests seien durchführbar, d.h. es gelte $D \neq \{\}$ bzw. $E'^0_M = \{\}$.

Dann gilt für die nach Definition 3.12 berechnete Menge E_E und die nach Definition 4.10 ermittelten Mengen $E_C^1, E_C^2, \ldots, E_C^g$ mit der Wahrscheinlichkeit $p_E(t)$:

$$E_E = E_C^1 \cup E_C^2 \cup \ldots \cup E_C^g$$

Beweis:
Nach Definition 3.12 gilt $E_B := G \setminus E_E$, daraus folgt $E_E := G \setminus E_B$. Ferner gilt nach Satz 4.27 $E_B = E_N$, d.h. $E_E = G \setminus E_N$

Es genügt also,

$$G \setminus E_N = E_C^1 \cup E_C^2 \cup \ldots \cup E_C^g$$

zu zeigen.

Nach Satz 4.11 sind in E_N genau die Teilnehmer enthalten, die nicht zur Rekonstruktion beitragen. In $G \setminus E_N$ sind folglich genau diejenigen Teilnehmer enthalten, die an der Rekonstruktion beteiligt sind.

Im folgenden wird gezeigt, dass auch in $E_C^1 \cup E_C^2 \cup \ldots \cup E_C^g$ alle Teilnehmer und nur Teilnehmer enthalten sind, die an der Rekonstruktion beteiligt sind.

Nach den Sätzen 4.13 und 4.20 sind alle zur Rekonstruktion beitragenden Teilnehmer bei Durchführung des erweiterten Tests auf Konsistenz in mindestens einer der Mengen $E'^1_M, E'^2_M, \ldots, E'^{|G|}_M, E_C^1, E_C^2, \ldots, E_C^g$ enthalten. Andere Teilnehmer (die nicht an der Rekon-

struktion mitwirken) sind nach Definition 4.10 in diesen Mengen $E'^{1}_{M}, E'^{2}_{M}, \ldots, E'^{|G|}_{M}$, $E^{1}_{C}, E^{2}_{C}, \ldots, E^{g}_{C}$ nicht enthalten. Es bleibt also zu zeigen, dass

$$E'^{1}_{M} \cup E'^{2}_{M} \cup \ldots \cup E'^{|G|}_{M} = \{\}.$$

Da Threshold Schemes betrachtet werden, bedeutet die Voraussetzung $E'^{0}_{M} = \{\}$, dass mindestens ein ehrlicher Teilnehmer mehr in G ist, als zur Rekonstruktion erforderlich ist. Daraus folgt, dass es nach Definition 2.10 in G kein minimales Compartment gibt (d.h.: das einzige beteiligte Compartment ist nicht minimal). Folglich gilt nach Satz 4.13 $E'^{1}_{M} \cup E'^{2}_{M} \cup \ldots \cup E'^{|G|}_{M} = \{\}$. Jeder an der Rekonstruktion beteiligte Teilnehmer ist also in $E^{1}_{C} \cup E^{2}_{C} \cup \ldots \cup E^{g}_{C}$ enthalten.

Da sowohl in $E^{1}_{C} \cup E^{2}_{C} \cup \ldots \cup E^{g}_{C}$ als auch in $G \setminus E_{N}$ genau alle an der Rekonstruktion beteiligten Teilnehmer enthalten sind, folgt:

$$E^{1}_{C} \cup E^{2}_{C} \cup \ldots \cup E^{g}_{C} = G \setminus E_{N}$$

und insgesamt

$$E_{E} = E^{1}_{C} \cup E^{2}_{C} \cup \ldots \cup E^{g}_{C}$$

Anmerkung:
Da die Mengen $E^{1}_{C}, E^{2}_{C}, \ldots, E^{g}_{C}$, welche nichtleer sind, nach Satz 4.20 alle Teilnehmer eines Compartments enthalten und ferner ein Threshold Scheme nur ein Compartment enthält, gilt

$$E^{i}_{C} = E_{E}$$

für alle i mit $E^{i}_{C} \neq \{\}$.

Insgesamt stellt der erweiterte Test auf Konsistenz für Threshold Schemes einen Spezialfall des Tests nach Definition 4.10 dar.

5. Multilevel Schemes

Die Multilevel Schemes wurden mit Definition 2.7 eingeführt. Es handelt sich um Secret Sharing Schemes, bei denen den Teilnehmern verschiedene Kompetenzniveaus, nämlich die Levels $l(P)$, zugeteilt werden. Je niedriger das Level, desto weniger Teilnehmer werden für die Rekonstruktion benötigt (d.h. desto höher die Kompetenz). Ein Teilnehmer des Levels l_j kann in einer zulässigen Teilnehmerkonstellation durch einen anderen Teilnehmer eines Levels $l \leq l_j$ ersetzt werden.

P^j ist nach Definition 2.7 die Menge aller Teilnehmer, deren Level kleiner gleich l_j ist ($P^j = \{P \in \mathcal{P} \mid l(P) \leq l_j\}$) und n_j ist die Anzahl dieser Teilnehmer ($n_j := |P^j|$).

Ähnlich wie für die Compartment Schemes gibt es auch für die Multilevel Schemes eine geometrische Realisierung, die der Realisierung für Threshold Schemes aus Definition 3.2 entspricht. Beispielsweise ist es möglich, den Teilnehmern entsprechend ihrem Level unterschiedlich viele Teilgeheimnisse zuzuordnen. Ein Teilnehmer mir hoher Kompetenz erhält dann mehr Teilgeheimnisse als ein Teilnehmer mit niedrigerer Kompetenz. Diese Realisierung hat jedoch zwei wesentliche Nachteile:

- An der Anzahl der Teilgeheimnisse ist das Level eines Teilnehmers ablesbar.
- Je nach Konstellation müssen deutlich mehr Teilgeheimnisse generiert werden als für den Fall, dass jedem Teilnehmer nur ein Teilgeheimnis zugeteilt wird.

Die im folgenden Abschnitt definierte geometrische Realisierung für Multilevel Schemes gewährleistet, dass eine Kontrollinstanz den Zugriff überprüfen kann und jedem Teilnehmer nur ein Teilgeheimnis zugeordnet wird.

5.1 Geometrische Multilevel Schemes

In Kapitel 3.1 wurden geometrische Secret Sharing Schemes im allgemeinen und die geometrischen Threshold Schemes im speziellen definiert. Im folgenden werden die Bezeichnungen der Definitionen 2.9 und 3.1 verwendet.

5.1 Definition: GEOMETRISCHE MULITLEVEL SCHEMES

Ein *geometrisches* ($l_1, l_2, \ldots, l_t$)*-Multilevel Scheme* wird als geometrisches Secret Sharing Scheme wie in Definition 3.1 realisiert [Ker92], für die Dimension d des projektiven Raumes PG(d, q) gelte:

$$d := l_t - 1 + s$$

Die Menge $\mathcal{B}$ der Blöcke seien alle linearen Unterräume von PG(d, q), die $\mathcal{K}$ in genau einem Punkt treffen und deren Rang in $\mathcal{L} = \{l_1, l_2, \ldots, l_t\}$ liegt.

Ferner sind gegeben:

- $B_0 := \left\{ B \in \mathcal{B} \;\middle|\; \kappa(B) := B \cap K = \{K_0\} \right\}$
- Innerhalb von B_0 lineare Unterräume $B_1, B_2, \ldots, B_t$ mit
  1. $B_1 \leq B_2 \leq \ldots \leq B_t$ und
  2. rang $B_i = l_i$ für $i = 1, 2, \ldots, t$.
- In den linearen Unterräumen B_i jeweils eine Menge E_i von Punkten ($i = 1, 2, \ldots, t$), für die gilt:
  3. $K_0 \notin E_i$
  4. $|E_i| = n_i$
  5. $E_i \subseteq B_i \setminus B_{i-1}$
  6. Je l_i Punkte aus $E_i \cup \{K_0\}$ erzeugen den Unterraum B_i.
  7. Für jede Menge M von l_i Punkten aus $E_1 \cup E_2 \cup \ldots \cup E_i$ gibt es eine Menge $T \subseteq M$ für die gilt: $\langle T \rangle \in \{B_1, B_2, \ldots, B_i\}$
  8. Für jede Teilgeheimnismenge $Y \subseteq E_1 \cup E_2 \cup \ldots \cup E_t$ mit $|Y \cap E_i| < l_i$ für alle $i = 1, 2, \ldots, t$ gilt: Die Punkte von $Y \cup \{K_0\}$ sind in allgemeiner Lage in B_0.

Jeder Teilnehmer des Levels l_i erhält einen Punkt aus E_i als Teilgeheimnis. Die Teilgeheimnisse verschiedener Teilnehmer unterscheiden sich.

Anmerkung:
Jedes geometrische Multilevel Scheme ist perfekt [Ker92].

Nach den Bedingungen 1. und 2. der obigen Definition bilden die Unterräume $B_1, B_2, \ldots, B_t$ eine Kette von Unterräumen, wie sie in Abbildung 23 dargestellt ist.

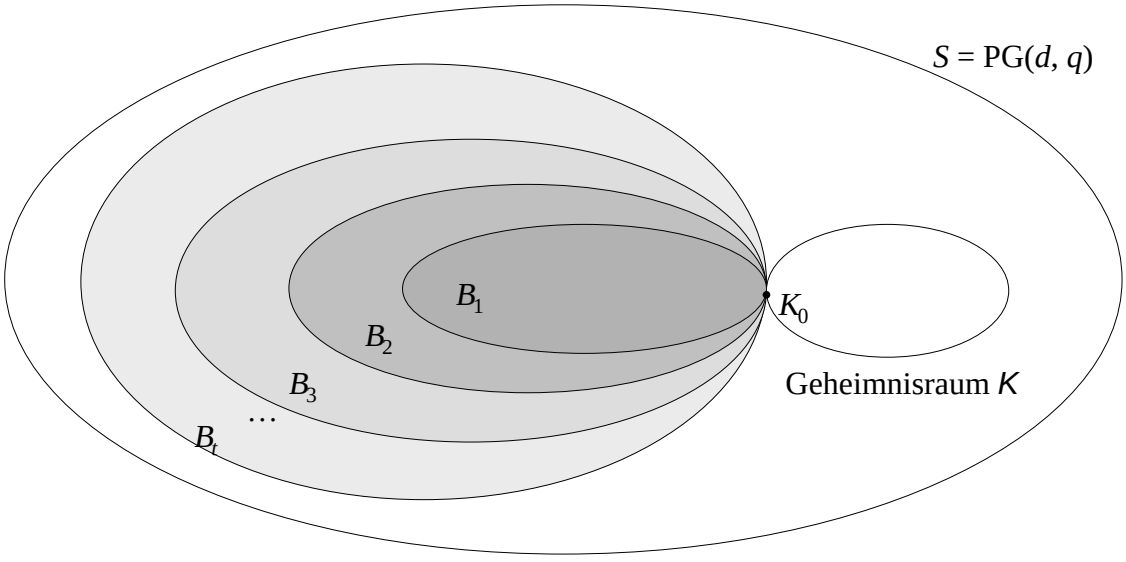


Abbildung 23: Unterraumkette für ein Multilevel Scheme mit t Levels

Ein Unterraum B, dessen Punkte an die Teilnehmer des Levels l verteilt werden, enthält alle Unterräume B' mit Teilgeheimnissen von Teilnehmern aus niedrigeren Levels. Daher ist gewährleistet, dass ein Teilnehmer eines Levels $l' < l$ bei der Rekonstruktion mit den Teilnehmern des Levels l zusammenwirken kann.

Bei der Rekonstruktion wird, wie bei den geometrischen Threshold und Compartment Schemes, das Erzeugnis der Teilgeheimnispunkte mit der Geheimnisgeraden geschnitten. Die folgende Abbildung zeigt ein $(2, 3)$-Multilevel Scheme in der geometrischen Realisierung.

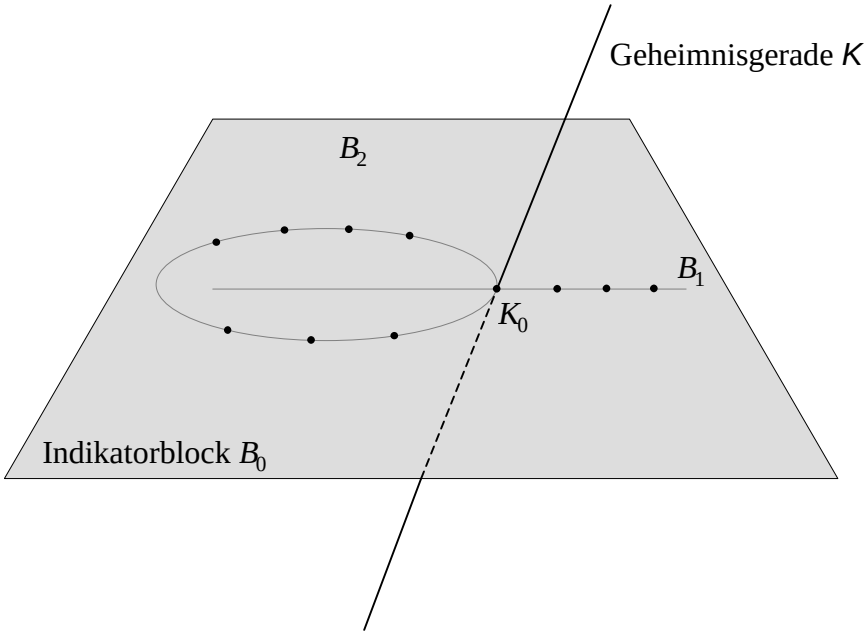


Abbildung 24: Ein geometrisches Multilevel Scheme

5.2 Erkennen eines Betruges

5.2.1 Test auf Konsistenz

Der Test auf Konsistenz für Threshold Schemes wurde in Kapitel 3.2, der für Compartment Schemes in Kapitel 4.2.1 vorgestellt. Ein entsprechender Test für Multilevel Schemes wird im folgenden dargestellt.

Zunächst wird die Kontrollstruktur für Multilevel Schemes definiert. Mit dieser Kontrollstruktur wird der Test auf Konsistenz durchgeführt.

5.2 Definition: KONTROLLSTRUKTUR FÜR MULTILEVEL SCHEMES

Seien $P = \{P_1, P_2, \ldots, P_n\}$ die Teilnehmer und $L = \{L_1, L_2, \ldots, L_t\}$ die Levels eines Multilevel Schemes wie in Definition 2.7.

Sei $l(P) \in L$ das Level des Teilnehmers $P \in P$. Eine Menge $\Phi \subseteq \mathbf{P}(P)$ mit

$$\Phi := \left\{ F \in \mathbf{P}(P) \;\middle|\; \text{es existiert ein } k \in L \text{ mit } \left| \left\{ P \in F \;\middle|\; l(P) \le k \right\} \right| \ge k+1 \right\}$$

heißt $(l_1, l_2, \ldots, l_t)$-*Multilevel-Scheme-Kontrollstruktur*.

In der Kontrollstruktur Φ ist im Vergleich zur Zugriffsstruktur für Multilevel Schemes aus Definition 2.7 in jeder Teilnehmermenge $F \in \Phi$ mindestens ein Teilnehmer mehr enthalten, als zur Rekonstruktion benötigt wird.

Vor der Definition des Tests auf Konsistenz für Multilevel Schemes wird noch eine Hilfsgröße, das Optimumlevel einer Teilnehmermenge, eingeführt.

5.3 Definition: OPTIMUMLEVEL EINER TEILNEHMERMENGE

Sei $G \in \Gamma$ eine zulässige Teilnehmermenge eines Multilevel Schemes. n_i sei wie in Definition 2.7 die Anzahl der Teilnehmer in G, deren Level kleiner gleich l_i ist.

Ein Level l_o, für welches

$$n_o - l_o = \max_i \left[n_i - l_i \right]$$

gilt, heißt *Optimumlevel der Teilnehmermenge G*.

Ein Level $l \in L$ wird nach Definition 5.3 genau dann als optimal bezeichnet, wenn die Differenz zwischen

- den an der Rekonstruktion beteiligten und
- den zur Rekonstruktion benötigten Teilnehmern

für kein anderes Level $l' \neq l$ größer ist als für l. Für ein Optimumlevel gibt es folglich maximal viele Teilnehmer, die auf Konsistenz geprüft werden können.

Anmerkung:
Zu einer Teilnehmermenge können mehrere Optimumlevel existieren.

5.4 Definition: TEST AUF KONSISTENZ (MULTILEVEL SCHEMES)

Sei $F \in \Phi$ die Kontrollstruktur eines Multilevel Schemes und l_o nach Definition 5.3 ein Optimumlevel von F. Sei wie in Definition 2.7

$$P^o := \left\{ P \in F \;\middle|\; l(P) \le l_o \right\}$$

und n_o die Anzahl der Teilnehmer, deren Level kleiner gleich l_o ist.

Betrachtet werden alle l_o-elementigen Teilmengen F_i von P^o. Die Anzahl dieser Mengen sei

$$f := \binom{n_o}{l_o}.$$

Für jede Teilmenge F_i (i = 1, 2, …, f) werden die Mengen K_i und B_i wie folgt gebildet:

$$B_i := \left\{ B \in \mathcal{B} \,\middle|\, \left(\alpha_K(F_i), B\right) \in \beta \right\}$$

$$K_i := \left\{ K \in \mathcal{K} \,\middle|\, \kappa(b) = K \text{ für alle } b \in B_i \right\}$$

Die Menge F besteht den *Test auf Konsistenz* genau dann, wenn jedes K_i aus genau einem Element besteht und alle diese Elemente gleich sind.

In dem Test auf Konsistenz wird die Menge P^o, die Menge aller Teilnehmer, deren Level kleiner gleich l_o ist, betrachtet. Dabei ist l_o ein Optimumlevel nach Definition 5.3. Der Test prüft, ob alle zulässigen Untermengen von P^o dasselbe Geheimnis rekonstruieren.

Anmerkung:
Bei Betrachtung der Definition 5.4 stellt sich die Frage, ob die Sicherheit des Tests mit f, der Anzahl der l_o-elementigen Untermengen wächst. In diesem Fall hätte ein Optimumlevel in Definition 5.3 nicht als ein Level mit

$$n_o - l_o = \max_i (n_i - l_i),$$

sondern sinnvoller als ein Level mit

$$\binom{n_o}{l_o} = \max_i \binom{n_i}{l_i}$$

definiert werden sollen.

Die Sätze 3.18 und 4.20, die sich mit der Wahrscheinlichkeit des Entdeckens eines Betruges mit Hilfe des erweiterten Test auf Konsistenz befassen, zeigen jedoch, dass die Sicherheit des Secret Sharing Schemes nur davon abhängt, dass möglichst viele ehrliche Teilnehmer in G enthalten sind. Die Anzahl f der Teilmengen hat keinen direkten Einfluss auf die Anzahl der ehrlichen Teilnehmer. Da nicht mehr als l_o - 1 Betrüger in G

vorhanden sein dürfen, nimmt die Anzahl der a priori ehrlichen Teilnehmer und damit die Sicherheit des Systems mit wachsender Differenz n_o - l_o zu.

Zur Durchführung des oben dargestellten Tests auf Konsistenz werden folgende Informationen benötigt:

- Die Teilgeheimnisse der Teilnehmer,
- für jeden Teilnehmer das Level, zu dem er gehört, und
- die Schwellen l_i innerhalb der Levels.

Der Test ist daher in Bezug auf die in Kapitel 1.7 formulierte Zielsetzung, dem Secret Sharing Scheme solle möglichst über die Shadows der Teilnehmer hinaus keine weitere Information zur Verfügung gestellt werden, unbefriedigend.

5.2.2 Levels ermitteln

Der in Kapitel 4.2.3, Definition 4.10, eingeführte erweiterte Test auf Konsistenz kann in einer leicht modifizierten Form auch auf Multilevel Schemes angewendet werden. Der Test wird mit Definition 5.9 eingeführt, und durch die darauffolgenden Sätze wird die Bedeutung der einzelnen Schritte des Tests geklärt.

Zunächst wird anhand eines Beispiels der Aufbau der Minimalstruktur nach Definition 2.12 näher betrachtet. Gegeben sei ein (3,5,8)-Multilevel Scheme wie es in der folgenden Abbildung dargestellt ist:

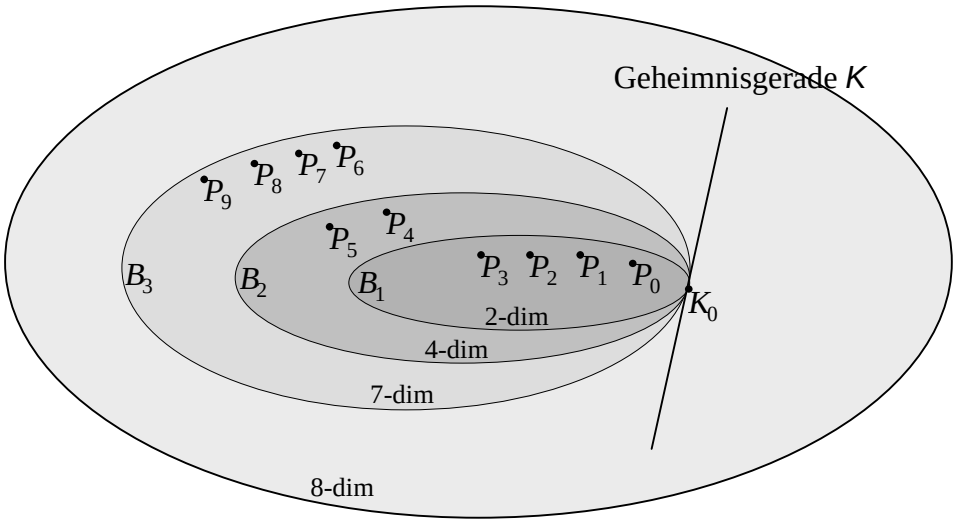


Abbildung 25: Ein (3, 5, 8)-Multilevel Scheme

Aus dem obigen Beispiel ergeben sich die folgenden zehn minimalen Mengen:

Block	Minimale Mengen
$\boldsymbol{B_1}$	$M_1 = \{P_0,P_1,P_2\}$, $M_2 = \{P_1,P_2,P_3\}$, $M_3 = \{P_2,P_3,P_0\}$, $M_4 = \{P_3,P_0,P_1\}$
$\boldsymbol{B_2}$	
$\boldsymbol{B_3}$	$M_5 = \{P_0,P_1,P_4,P_5,P_6,P_7,P_8,P_9\}$, $M_6 = \{P_0,P_2,P_4,P_5,P_6,P_7,P_8,P_9\}$, $M_7 = \{P_0,P_3,P_4,P_5,P_6,P_7,P_8,P_9\}$, $M_8 = \{P_1,P_2,P_4,P_5,P_6,P_7,P_8,P_9\}$, $M_9 = \{P_1,P_3,P_4,P_5,P_6,P_7,P_8,P_9\}$, $M_{10} = \{P_2,P_3,P_4,P_5,P_6,P_7,P_8,P_9\}$

Die erste Zeile der Tabelle enthält alle minimalen Mengen, die nur Teilnehmer aus B_1 enthalten. Das sind alle dreielementigen Untermengen von $\{P_1,P_2,P_3,P_4\}$.

Die zweite Zeile enthält alle minimalen Mengen, die sich mit Teilnehmern aus B_2 bilden lassen, wobei mindestens ein Teilnehmer aus $B_2 \setminus B_1$ in der minimalen Menge enthalten sein soll. In dem betrachteten (3,5,8)-Multilevel Scheme existieren keine solchen Mengen.

Schließlich enthält die dritte Zeile alle minimalen Mengen, die sich mit Teilnehmern aus B_3 bilden lassen, wobei mindestens ein Teilnehmer aus $B_3 \setminus B_2$ in der minimalen Menge enthalten sein soll. In dem Beispiel gibt es sechs solche Mengen.

Insgesamt ergibt sich folgendes:

- Es gibt vier minimale Mengen mit Teilnehmern aus B_1.
- Durch Hinzunahme der Teilnehmer, deren Teilgeheimnisse aus $B_2 \setminus B_1$ stammen, ergeben sich (im Vergleich zu B_1) keine weiteren minimalen Mengen.
- Durch Hinzunahme der Teilnehmer aus $B_3 \setminus B_2$ existieren sechs weitere minimale Mengen.

Im folgenden wird die Frage, woran es liegt, dass die Teilnehmer aus $B_2 \setminus B_1$ keine weiteren minimalen Mengen erzeugen, die Teilnehmer aus $B_3 \setminus B_2$ dies jedoch tun, betrachtet.

Aus B_2 (einschließlich B_1) werden zur Rekonstruktion mindestens fünf Teilnehmer benötigt. Jede fünfelementige Teilnehmermenge aus B_2 enthält in dem Beispiel mindestens drei Teilnehmer aus B_1, da es nur zwei Teilnehmer in $B_2 \setminus B_1$ gibt. Das bedeutet, dass keine der fünfelementigen Teilnehmermengen aus B_2 minimal ist, da sie nach Weglassen eines Teilnehmers aus $B_2 \setminus B_1$ zulässig bleibt.

Aus B_3 werden zur Rekonstruktion mindestens acht Teilnehmer benötigt. Es existieren genau sechs achtelementige Teilnehmermengen aus B_3, die weniger als drei Teilnehmer aus B_1 und weniger als fünf Teilnehmer aus B_2 enthalten. Diese Teilnehmermengen sind minimal.

5.5 Definition: PRÜFBARE UND NICHTPRÜFBARE LEVELS

Sei $G \in \Gamma$ eine zulässige Teilnehmermenge eines Multilevel Schemes. n_i sei nach Definition 2.7 die Anzahl der Teilnehmer in G, deren Level kleiner gleich l_i ist.

Ein Level l_i ($i = 1, 2, \ldots, t$) heißt *prüfbares Level*, wenn

$$n_i > l_i \text{ und}$$

$$n_i - n_k > l_i - l_k \quad \text{für } \textit{alle } k = 1, 2, \ldots, i - 1$$

gilt.

Ein Level heißt *nichtprüfbares Level*, wenn es kein prüfbares Level ist.

Nach der Definition heißt ein Level l_i prüfbar, wenn für alle höherwertigen Levels l_k gilt: Es sind mehr als ($l_i - l_k$) Teilnehmer in $P^i \setminus P^k$ enthalten.
Zum Verständnis wird noch einmal das obige Beispiel betrachtet. Dort gilt:

	l_i	n_i	$l_i - l_k$	$n_i - n_k$
$i = 1$	3	4		
$i = 2$ **$k = 1$**	5	6	2	2
$i = 3$ **$k = 2, 1$**	8	10	3, 5	4, 6

Die Level 1 und 3 sind also prüfbare Levels, während das Level 2 nichtprüfbar ist.

Anmerkung:
Nach der obigen Definition wird $n_i - n_k > l_i - l_k$ im Vergleich zu für *allen* höherwertigen Levels gefordert. In dem betrachteten Beispiel würde jedoch eine Prüfung lediglich für $k = i - 1$ bereits dasselbe Ergebnis erzielen. Das gilt jedoch nicht im allgemeinen. Beispielsweise ergibt sich für $l_1 = 3$, $l_2 = 5$ und $l_3 = 8$ mit $n_1 = 5$, $n_2 = 6$ und $n_3 = 10$ die Nichtprüfbarkeit des Levels l_3 erst durch den Vergleich mit dem Level l_1. Weil $l_3 - l_1 = 5 = n_3 - n_1$ gilt, lassen sich keine minimalen Mengen mit Teilnehmern aus $B_3 \setminus B_1$ finden. Der Vergleich von l_3 allein mit l_2 würde die Prüfbarkeitsbedingung nicht verletzen.

Das größte prüfbare Level einer Teilnehmermenge hat im Verlauf des erweiterten Tests auf Konsistenz für Multilevel Schemes eine wichtige Bedeutung, daher erhält es durch die folgende Definition einen Namen.

5.6 Definition: MAXIMUMLEVEL EINER TEILNEHMERMENGE

Sei $G \in \Gamma$ eine zulässige Teilnehmermenge eines Multilevel Schemes. Das *Maximumlevel* l_{max} von G ist das größte (d.h. niederwertigste) prüfbare Level.

Ferner sei:

$$n_{max} = \left| \left\{ P \in G \,\middle|\, l(P) \leq l_{max} \right\} \right|$$

Schließlich sei i_{max} der *Index des Maximumlevels*, d.h.

$$\text{wenn } l_j = l_{max} \text{ für } j \in \{1, \ldots, t\}, \text{ dann gilt: } i_{max} := j$$

Nach den Definitionen 5.5 und 5.6 gilt für das Maximumlevel:

$$n_{max} - n_k > l_{max} - l_k \quad \text{für alle } k < i_{max} \text{ und}$$

$$\text{für alle } l_i > l_{max} \text{ existiert mindestens ein } k < i \text{ mit } n_i - n_k \leq l_i - l_k.$$

Mit Hilfe des oben eingeführten Maximumlevels wird es möglich sein, notwendige und hinreichende Bedingungen dafür anzugeben, ob zu einem Teilnehmer P eine minimale Menge M mit $P \in M$ existiert. Satz 5.8 wird diese Bedingungen angeben. Das folgende Lemma wird den Beweis dieses Satzes vereinfachen. Es gibt an, unter welchen hinreichenden und notwendigen Bedingungen die gegebene Teilnehmermenge eines Multilevel Schemes minimal ist.

5.7 Lemma:

Sei $G \in \Gamma$ eine zulässige Teilnehmermenge eines Multilevel Schemes. G ist genau dann minimal, wenn alle folgenden Bedingungen erfüllt sind:

i) $n_i = l_i$ für ein $i \in \{1, \ldots, t\}$

ii) $l(P) \leq l_i$ für alle $P \in G$

iii) $n_j < l_j$ für $j = 1, 2, \ldots, i - 1$

Beweis:
Zu zeigen:

a) Sei eine Teilnehmermenge G mit den Voraussetzungen i), ii) und iii) gegeben. Dann ist G minimal.
b) Sei eine Teilnehmermenge G minimal, dann gelten die Bedingungen i), ii) und iii).

Zu a):
Wird ein Teilnehmer aus G entfernt, so verringert sich -wegen ii)- n_i um einen Teilnehmer. Daher gilt -wegen i) und iii)- $n_j < l_j$ für alle $j \in \{1, \ldots, t\}$ und die entstandene Teilnehmermenge ist nicht zulässig. Folglich ist G nach Definition 2.11 minimal.

Zu b):
Da G minimal ist, muss G nach Definition 2.11 nach Entfernen eines Teilnehmers unzulässig sein. Im folgenden wird gezeigt, dass daraus die Bedingungen i), ii) und iii) folgen.

Da G zulässig ist, muss für mindestens ein i gelten: $n_i \geq l_i$.
Ferner gilt, $n_i \leq l_i$ denn: Wäre $n_i > l_i$, so könnte ein Teilnehmer P mit $l(P) \leq l_i$ entfernt werden und die resultierende Teilnehmermenge wäre zulässig. Das wäre ein Widerspruch dazu, dass G minimal ist.
Insgesamt folgt $n_i = l_i$ und es gilt i).

Wäre in G ein Teilnehmer mit $l(P) > l_i$ enthalten, so könnte er weggelassen werden, und die resultierende Teilnehmermenge wäre zulässig. Das wäre ein Widerspruch dazu, dass G minimal ist. Daraus folgt $l(P) \leq l_i$ für alle Teilnehmer $P \in G$ und es gilt ii).

Würde $n_j \geq l_j$ (für ein $j < i$) gelten, so könnte ein Teilnehmer mit $l(P) > l_j$ weggelassen werden, und die resultierende Teilnehmermenge wäre zulässig. Auch das wäre ein Widerspruch dazu, dass G minimal ist. Daraus folgt $n_j < l_j$ für $j < i$ und es gilt iii).

Der nächste Satz sagt aus, dass zu einem Teilnehmer P genau dann (mindestens) eine minimale Menge M mit $P \in M$ existiert, wenn P aus einem Level stammt, das dem Maximumlevel mindestens gleichwertig ist.

5.8 Satz:

Sei $G \in \Gamma$ eine zulässige Teilnehmermenge eines Multilevel Schemes. Ferner sei l_{max} nach Definition 5.6 das Maximumlevel von G. Betrachtet werde ein Teilnehmer $P \in G$ mit $l(P) = l_i$. Es gilt:

Eine minimale Menge M mit $P \in M$ existiert genau dann, wenn $l_i \leq l_{max}$ gilt.

Beweis:
Sei $P \in G$ mit $l(P) = l_i$. Zu zeigen:
a) Es existiert eine minimale Menge M mit $P \in M \Rightarrow l_i \leq l_{max}$.
b) $l_i \leq l_{max} \Rightarrow$ Es existiert eine minimale Menge M mit $P \in M$.

Zu a):
Sei eine minimale Menge M von G gegeben. Dann gilt nach Lemma 5.7 für M und ein j: $|M| = l_j$. Ferner sei $P \in M$, d.h.: $l(P) = l_i \leq l_j$.

Der Beweis erfolgt nun indirekt: Sei $l_i > l_{max}$.
Dann gilt $l_j > l_{max}$. Das bedeutet nach den Definitionen 5.5 und 5.6, dass ein $k < j$ mit $n_j - n_k \leq l_j - l_k$ existiert. Im folgenden wird gezeigt, dass M aus diesem Level k mindestens l_k Teilnehmer enthält. Diese Teilnehmer könnten das Geheimnis nach Definition 2.7

rekonstruieren. Da aber $|M| = l_j > l_k$ gilt, wäre dann M nach Lemma 5.7 keine minimale Menge.

Die Teilnehmer in M lassen sich in zwei Klassen aufteilen, nämlich Teilnehmer aus P^k und Teilnehmer, die nicht aus P^k stammen. Die Anzahl der Teilnehmer in M, die nicht aus P^k stammen, ist höchstens $|P^j| - |P^k| = n_j - n_k$. Es gilt:

$$n_j - n_k \leq l_j - l_k = |M| - l_k$$

In M sind also höchstens $|M| - l_k$ Teilnehmer enthalten, die nicht aus P^k stammen. Folglich stammen die übrigen mindestens l_k Teilnehmer von M aus P^k.

Sei $M' := M \cap P^k$. Dann gilt: $|M'| = |M \cap P^k| \geq l_k$. Es existiert folglich eine zulässige Teilnehmermenge $M' \subset M$ und M ist keine minimale Menge. Wegen des Widerspruchs gilt also $l_i \leq l_{max}$.

Zu b):
Aus $l_i \leq l_{max}$ folgt, dass für ein $j \geq i$ gilt: $n_j - n_k > l_j - l_k$ für alle $k < j$. Im folgenden wird gezeigt, dass mit dieser Voraussetzung eine Menge M mit den Eigenschaften

i) $P \in M$, und

ii) M ist minimal, d.h. nach Lemma 5.7

- α) $|M \cap P^j| = l_j$ für ein $j \in \{1, \ldots, t\}$,
- β) $l(P) \leq l_j$ für alle $P \in M$ und
- γ) $|M \cap P^k| < l_k$ für $k < j$.

existiert.

Eine Menge M, die den Eigenschaften i), ii)α) und ii)β) entspricht, lässt sich trivial erzeugen. Im folgenden wird gezeigt, dass diese so gewählt werden kann, dass sie auch der Eigenschaft ii)γ) entspricht.

Für alle $k < j$ gilt:
In G sind n_k Teilnehmer mit $l(P) \leq l_k$ (und n_j Teilnehmer mit $l(P) \leq l_j$) enthalten. Folglich kann M so konstruiert werden, dass $(n_j - n_k)$ Teilnehmer in M enthalten sind, die *nicht* aus P^k stammen. Die Anzahl der Teilnehmer in M, die aus P^k stammen, ist dann:

$$|M| - (n_j - n_k).$$

Insgesamt folgt (mit $n_j - n_k > l_j - l_k$), dass M so gewählt werden kann, dass

$$|M \cap P^k| = |M| - (n_j - n_k) = l_j - (n_j - n_k) < l_k$$

gilt. Damit ist die Eigenschaft ii)γ) für diese Menge M erfüllt.

M ist also nach Lemma 5.7 eine minimale Menge und es gilt $P \in M$.

Anmerkung:
Nach Voraussetzung des Satzes ist l_{max} das Maximumlevel von $G \in \Gamma$. Dadurch wird implizit vorausgesetzt, dass überhaupt ein prüfbares Level existiert.

Nach diesen Vorbetrachtungen zur Struktur der minimalen Mengen wird nun der erweiterte Test auf Konsistenz für Multilevel Schemes definiert.

5.9 Definition: ERWEITERTER TEST AUF KONSISTENZ (MULTILEVEL SCHEMES)

Sei $G \in \Gamma$ eine zulässige Teilnehmermenge eines Multilevel Schemes. Seien $M_1, M_2, \ldots, M_m$ die Mengen der Minimalstruktur M von G mit $|M| > 1$.

Der *erweiterte Test auf Konsistenz* besteht aus 3 Teilen:

Teil I:
Aus der Minimalstruktur M werden zwei Ergebnismengen gebildet:

$$E'^{0}_{\mathrm{M}} := \left\{ P \in G \,\middle|\, P \in M_i \text{ für alle } i = 1, 2, \ldots, m \right\}$$

$$E_{\mathrm{N}} := \left\{ P \in G \,\middle|\, P \notin M_i \text{ für alle } i = 1, 2, \ldots, m \right\}$$

Der erweiterte Test auf Konsistenz heißt *durchführbar*, wenn

$$E'^{0}_{\mathrm{M}} = \{\}$$

gilt.

Teil II:
Für jede minimale Menge M_i werden die Mengen B_i und K_i wie folgt gebildet:

$$B_i := \left\{ B \in \mathcal{B} \,\middle|\, \left(\alpha_K(M_i), B\right) \in \beta \right\}$$

$$K_i := \left\{ K \in \mathcal{K} \,\middle|\, \kappa(b) = K \text{ für alle } b \in B_i \right\}$$

Die Menge G besteht den *erweiterten Test auf Konsistenz* genau dann, wenn jedes K_i aus genau einem Element besteht und alle diese Elemente gleich sind.

Teil III:
Sei c_k (für $k = 0, 1, \ldots, |G|$) die Anzahl aller Prüfstrukturen einer Ordnung kleiner gleich k, d.h. mit den Bezeichnungen aus Definition 4.7

$$c_k = \sum_{i=0}^{k} g_i.$$

Für die nichtleeren Prüfstrukturen der Ordnung $k = 1, 2, \ldots, |G|$ werden sukzessiv die Ergebnismengen derselben Ordnung wie folgt gebildet:

$$E_{c_{k-1}+1} := \left\{ P \in G \middle| P \notin M \text{ für alle } M \in \underline{M}_{c_{k-1}+1} \right\} \setminus R_k$$
$$\vdots$$
$$E_{c_k} := \left\{ P \in G \middle| P \notin M \text{ für alle } M \in \underline{M}_{c_k} \right\} \setminus R_k$$

Die Mengen R_k sind rekursiv definiert als

$$R_1 = E_{\mathrm{N}}$$

und für $k \geq 2$

$$R_k := R_{k-1} \cup \left(\bigcup_{j=c_{k-2}+1}^{c_{k-1}} E_j \right) = E_{\mathrm{N}} \cup \left(\bigcup_{j=1}^{c_{k-1}} E_j \right).$$

Aus diesen Mengen werden die Vereinigungsmengen E_{L}^j $(1 \leq j \leq g)$ wie folgt gebildet:

$$E_{\mathrm{L}}^1 := \begin{cases} E_1 \text{ wenn } E_1 \supset G_1 \\ \{\,\} \text{ wenn } E_1 \subseteq G_1 \end{cases}$$
$$\vdots$$
$$E_{\mathrm{L}}^g := \begin{cases} E_g \text{ wenn } E_g \supset G_g \\ \{\,\} \text{ wenn } E_g \subseteq G_g \end{cases}$$

Die Mengen G_i $(i = 1, \ldots, g)$ sind die Prüfmengen zu G nach Definition 4.7.

Der Test unterscheidet sich lediglich in Teil III von dem Test für Compartment Schemes. Dieser Teil des Testes muss für die Multilevel Schemes nicht (wie bei den Compartment Schemes) in zwei Schritte unterteilt werden.

Die verschiedenen Mengen des erweiterten Testes auf Konsistenz werden im folgenden untersucht.

5.10 Satz:

Sei $G \in \Gamma$ eine zulässige Teilnehmermenge eines Multilevel Schemes und P ein Teilnehmer aus G. Der erweiterte Test auf Konsistenz werde nach Definition 5.9 durchgeführt. Dann gilt:

$$P \in E_{\mathrm{N}} \Leftrightarrow l(P) > l_{max}.$$

Beweis:
Diese Aussage folgt sofort aus Definition 5.9 und Satz 5.8.

Die Teilnehmer, die in E_N enthalten sind, kommen nach Definition 5.9 in keiner minimalen Menge vor. Solche Teilnehmer können durch den oben definierten Test nicht auf Konsistenz geprüft werden. Satz 5.10 besagt, dass alle diese nicht kontrollierbaren Teilnehmer aus Levels stammen, die niederwertiger sind als das Maximumlevel.

Der nächste Satz klärt, warum $E'^{0}_{M} = \{\}$ Voraussetzung für die Durchführbarkeit des Testes ist. Es wird gezeigt: Genau wenn $E'^{0}_{M} \neq \{\}$, dann existiert kein Level l_i, von welchem mehr als l_i Teilnehmer in G vertreten sind.

5.11 Satz:

Sei $G \in \Gamma$ eine zulässige Teilnehmermenge eines Multilevel Schemes. Der erweiterte Test auf Konsistenz werde nach Definition 5.9 durchgeführt. Dann gilt:

$$E'^{0}_{M} \neq \{\} \quad \Leftrightarrow \quad n_i \leq l_i \text{ für alle } 1 \leq i \leq t$$

Nach Definition 2.7 ist t der Index des niederwertigsten Levels.

Beweis:
Zu zeigen:

a) $E'^{0}_{M} \neq \{\} \quad \Rightarrow \quad n_i \leq l_i$ für alle $1 \leq i \leq t$
   Gezeigt wird: $n_i > l_i$ für mindestens ein $i \Rightarrow E'^{0}_{M} = \{\}$

b) $n_i \leq l_i$ für alle $1 \leq i \leq t \quad \Rightarrow \quad E'^{0}_{M} \neq \{\}$

Zu a):
Sei $n_i > l_i$ für mindestens ein i. Sei ferner l_j das kleinste (d.h. höchstwertige) Level mit $n_j > l_j$. Im folgenden wird gezeigt, dass

i) sowohl für alle P mit $l(P) \leq l_j$
ii) als auch für alle P mit $l(P) > l_j$

minimale Mengen existieren, die P nicht enthalten. Da E'^{0}_{M} nach Definition 5.9 Teilnehmer enthält, die in jeder minimalen Mengen vorkommen, würde daraus folgen: $E'^{0}_{M} = \{\}$.

Zu i):
Sei P gegeben mit $l(P) \leq l_j$
Für alle $k < j$ gilt: $n_k \leq l_k$. Daraus folgt:

$$n_j - n_k \geq n_j - l_k > l_j - l_k$$

Das bedeutet nach Definition 5.6: $l_j \leq l_{max}$, und daraus folgt nach Satz 5.8: Für jeden Teilnehmer $P \in P^j$ (d.h. $l(P) \leq l_j$) existiert eine minimale Menge M mit $P \in M$.

Sei also eine minimale Menge M gegeben mit $P \in M$. Sei $|M| = l_j$; das ist möglich, da $n_j > l_j$ und $n_k \leq l_k$ für $k < j$. Ferner sei P' gegeben mit $P' \notin M$ und $l(P') = l_j$ (einen solchen Teilnehmer gibt es, da $n_j > l_j$). Sei $M' := (M \cup \{P'\}) \setminus \{P\}$. Dann ist M' einen minimale Menge mit $P \notin M'$.

Zu ii):
Sei P gegeben mit $l(P) > l_j$.
Dann gilt für die in i) konstruierte minimale Menge M: $P \notin M$.

Insgesamt folgt: Da für jeden Teilnehmer P eine minimale Menge M existiert, die P nicht enthält, gilt

$$E'^{0}_{M} = \{\}.$$

Zu b):
Da $G \in \Gamma$ eine zulässige Teilnehmermenge eines Multilevel Schemes ist, muss für mindestens ein i gelten: $n_i \geq l_i$. Sei j das kleinste dieser i:

Im folgenden wird gezeigt, dass mit der Voraussetzung „$n_i \leq l_i$ für alle $1 \leq i \leq t$“ zu G nur *eine* minimale Menge M existiert, nämlich

$$M = \left\{ P \in P \;\middle|\; l(P) = l_j \right\}.$$

Daraus würde folgen: $E'^{0}_{M} = M \neq \{\}$

i) Zu zeigen: M ist eine minimale Menge.
Die Aussage folgt nach Lemma 5.7, denn es gilt nach Voraussetzung

α) $n_j = l_j$
β) $l(P) \leq l_j$ für alle $P \in M$ und
γ) $n_k < l_k$ für alle $k = 1, 2, \ldots, j - 1$

ii) Zu zeigen: Alle anderen Teilmengen von G sind nicht minimal.
Sei $M' \subseteq G$ eine zulässige Teilnehmermenge. Dann muss in M' für ein $k \in \{1, 2, \ldots, t\}$ gelten: $n_k \geq l_k$. Nach Voraussetzung des Satzes gilt $n_k \leq l_k$, insgesamt gilt also $n_k = l_k$. Ferner sei $k \neq j$, damit $M' \neq M$.

α) Sei $k < j$:
Nach der Definition von j gilt für $k < j$: $n_k < l_k$. Eine zulässige Teilnehmermenge M' existiert also für $k < j$ nicht.

β) Sei $k > j$:
Da in G nach Voraussetzung (nur) n_k Teilnehmer P mit $l(P) \leq l_k$ vertreten sind, müssen alle (nach Vereinbarung in G vorhandenen) n_j Teilnehmer mit $l(P) \leq l_j$ in M' enthalten sein. Folglich gilt $M \subset M'$. Da M eine zulässige Teilnehmermenge ist, kann M' keine minimale Menge sein.

Wegen $k \neq j$ folgt insgesamt:

$$E'^{0}_{M} \neq \{\}$$

Nach obigem Satz gilt: Wenn $E'^{0}_{M} \neq \{\}$, dann existiert kein nach Definition 5.5 prüfbares Level und der Test auf Konsistenz ist nicht durchführbar.

Insgesamt ist die Bedeutung des Teil I des Testes geklärt. Teil II des Testes entspricht dem mit Definition 5.4 eingeführten Test. Die Rekonstruktionsergebnisse aller minimalen Mengen von *G* werden miteinander verglichen. Wenn alle rekonstruierten Mengen aus einem Element bestehen und alle diese Mengen gleich sind, wird der Konsistenztest bestanden.

Bevor Teil III des erweiterten Tests auf Konsistenz für Multilevel Schemes durch einige Sätze näher beleuchtet wird, ist es zweckmäßig, die Teilnehmer der nichtprüfbaren Levels (Definition 5.5) noch einmal näher zu betrachten.

Aus dem in Abbildung 25 (Seite 104) dargestellten Beispiel wird die Bedeutung dieser Teilnehmer ersichtlich. Die Teilnehmer aus B_1 und B_3 stammen aus prüfbaren Levels, die Teilnehmer aus B_2 nicht. Die Teilnehmer aus B_2 wirken in der betrachteten Teilnehmermenge lediglich mit dem Kompetenzniveau eines Teilnehmers aus B_3. Das heißt mit anderen Worten: Würden die beiden Teilnehmer aus B_2 durch zwei zusätzliche Teilnehmer aus B_3 ersetzt, so würde sich an dem Rekonstruktionsergebnis und am Verlauf des Testes auf Konsistenz nichts ändern. Dieser Sachverhalt wird durch den folgenden Satz bestätigt.

5.12 Satz:

Sei $G \in \Gamma$ eine zulässige Teilnehmermenge eines Multilevel Schemes. l_i sei ein nach Definition 5.5 nichtprüfbares Level, l_j sei das nächstniederwertige prüfbare Level. Betrachtet werde ein Teilnehmer *P* mit $l(P) = l_i$.

Dann ist *P* in genau denselben minimalen Mengen enthalten, in denen er enthalten wäre, wenn $l(P) = l_j$ gelten würde.

Beweis:
Zu zeigen:

a) Sei $l(P) = l_i$, $P \in M$ und *M* eine minimale Menge von *G*. Es wird gezeigt, dass *M* auch dann eine minimale Menge ist, wenn $l(P) = l_j$ gilt.

b) Sei $l(P) = l_j$, $P \in M$ und *M* eine minimale Menge von *G*. Es wird gezeigt, dass *M* auch dann eine minimale Menge ist, wenn $l(P) = l_i$ gilt.

Zu a):
Nach Lemma 5.7 gilt für eine minimale Menge M:

i) $n_k = l_k$ für ein $k \in \{1, \ldots, t\}$

ii) $l(P) \leq l_k$ für alle $P \in M$

iii) $n_m < l_m$ für $1 \leq m < k$

Da l_i ein nichtprüfbares und l_j das nächstniederwertige prüfbare Level ist, muss nach Satz 5.8 in Bedingung i) für M mit $P \in M$ gelten: $k \geq j$. Sei nun $l(P) = l_j$. Dadurch wird jeweils n_m, die Anzahl der Teilnehmer des Levels l_m verändert. Diese neue Anzahl werde mit n_m' bezeichnet. Es gilt:

m	$1 \leq m < i$	$i \leq m < j$	$j \leq m \leq k$
n_m'	$n_m' = n_m$	$n_m' = n_m - 1$	$n_m' = n_m$

Da sich die Anzahl der Teilnehmer des Levels l_k (mit $k \geq j$) nicht verändert hat, gilt nach wie vor i). Aus $k \geq j$ folgt auch ii) und aus $n_m' \leq n_m$ für alle $m \leq k$ folgt iii). Nach Satz 5.7 ist folglich M nach wie vor eine minimale Menge von G.

Zu b):
Nach Lemma 5.7 gelten die obigen Bedingungen i), ii) und iii). Da $P \in M$ und $l(P) = l_j$ muss $k \geq j$ gelten. Sei nun $l(P) = l_i$. Die neue Anzahl der Teilnehmer pro Level werde erneut mit n_m' bezeichnet. Es gilt:

m	$1 \leq m < i$	$i \leq m < j$	$j \leq m \leq k$
n_m'	$n_m' = n_m$	$n_m' = n_m + 1$	$n_m' = n_m$

Die Bedingungen i) und ii) werden offensichtlich auch für $l(P) = l_i$ erfüllt. Im folgenden wird gezeigt, dass Bedingung iii) insbesondere für die Level, in denen $n_m' > n_m$ gilt (das sind die Levels l_i bis l_{j-1}), erfüllt ist. Zunächst wird l_i betrachtet. Da l_i nichtprüfbar ist, (nach Voraussetzung des Satzes auch nicht für $l(P) = l_i$,) gilt nach Definition 5.5 für mindestens ein $m < i$: $n_i' - n_m \leq l_i - l_m$. Ferner gilt für dieses $m < i$ nach iii), da M eine minimale Menge ist: $n_m < l_m$. Daraus folgt:

$$n_i' \leq l_i - l_m + n_m < l_i - l_m + l_m = l_i, \text{ also } n_i' < l_i$$

Diese Überlegung gilt analog für die anderen Levels l_{i+1} bis l_{j-1}. Demnach ist auch Bedingung iii) erfüllt.

Insgesamt gelten also auch für $l(P) = l_i$ die obigen Bedingungen i), ii) und iii) und nach Satz 5.7 ist M nach wie vor eine minimale Menge von G.

Bei dem Test auf Konsistenz werden ausschließlich minimale Mengen betrachtet. Diese minimalem Mengen bleiben nach Satz 5.12 unverändert, wenn den Teilnehmern eines nicht prüfbaren Levels das nächstniederwertige prüfbare Level zugeordnet wird. Der Verlauf des Testes wird dadurch folglich nicht beeinflusst.

Im folgenden wird davon ausgegangen, dass alle Levels einer Teilnehmermenge, die höherwertiger als das Maximumlevel sind, prüfbare Levels sind. Das ist nach den obigen Überlegungen zulässig.

Nun wird der minimale Überhang eines Levels eingeführt. Er wird die Formulierung der darauffolgenden Sätze vereinfachen.

5.13 Definition: MINIMALER ÜBERHANG DES LEVELS l_i

Sei $G \in \Gamma$ eine zulässige Teilnehmermenge eines Multilevel Schemes. Der *minimale Überhang* $\ddot{U}_i$ *des Levels* l_i *in* G ist definiert als:

$$\ddot{U}_i := \min_{k<i} [(n_i - n_k) - (l_i - l_k)] \text{ (für } i \geq 2)$$

$$\text{und } \ddot{U}_1 := n_1 - l_1$$

Insbesondere ist $\ddot{U}_{max}$ der minimale Überhang des Maximumlevels l_{max}.

Wenn die Teilnehmermenge, wie oben vereinbart, nur prüfbare Levels enthält, kann der minimale Überhang einfacher dargestellt werden, wie der folgende Satz zeigt.

5.14 Satz:

Sei $G \in \Gamma$ eine zulässige Teilnehmermenge eines Multilevel Schemes. Alle Levels $l_i \leq l_{max}$ seien nach Definition 5.5 prüfbar.

Dann gilt für den minimalen Überhang $\ddot{U}_i$ des Levels $l_i \leq l_{max}$ (für $i \geq 2$):

$$\ddot{U}_i := (n_i - n_{i-1}) - (l_i - l_{i-1})$$

Beweis:
Nach Definition 5.13 gilt für $i \geq 2$:

$$\begin{aligned}
\ddot{U}_i &= \min_{k<i} [(n_i - n_k) - (l_i - l_k)] \\
&= \min_{k<i} [(n_i - n_{i-1} + n_{i-1} - n_k) - (l_i - l_{i-1} + l_{i-1} - l_k)] \\
&= \min_{k<i} [(n_{i-1} - n_k) - (l_{i-1} - l_k) + (n_i - n_{i-1}) - (l_i - l_{i-1})] \\
&= \min_{k<i} [(n_{i-1} - n_k) - (l_{i-1} - l_k)] + (n_i - n_{i-1}) - (l_i - l_{i-1})
\end{aligned}$$

Da nach Voraussetzung alle Level prüfbar sind, gilt nach Definition 5.5:

$$n_{i-1} - n_k > l_{i-1} - l_k \text{ (für alle } k < i\text{-}1)$$

Daher wird der obige Ausdruck für $k = i$-1 minimal und es gilt

$$\ddot{U}_i = (n_i - n_{i-1}) - (l_i - l_{i-1})$$

Das folgende Lemma ist eine einfache Folgerung aus Satz 5.14. Es wird in den Beweisen der späteren Sätze genutzt.

5.15 Lemma:

Sei $G \in \Gamma$ eine zulässige Teilnehmermenge eines Multilevel Schemes. Alle Levels $l_i \leq l_{max}$ seien nach Definition 5.5 prüfbar.

Dann gilt für die Anzahl n_i der Teilnehmer P mit $l(P) \leq l_i$:

$$n_i = l_i + \sum_{j=1}^{i} \ddot{U}_j$$

Beweis:
Für $i = 1$ folgt die Aussage sofort aus Definition 5.13.

Sei $i \geq 2$. Nach Satz 5.14 gilt:

$$\sum_{j=1}^{i} \ddot{U}_j = n_1 - l_1 + \sum_{j=2}^{i} [(n_j - n_{j-1}) - (l_j - l_{j-1})]$$

$$= n_1 - l_1 + n_i - n_1 - l_i + l_1$$

$$= n_i - l_i$$

Daraus folgt $n_i = l_i + \sum_{j=1}^{i} \ddot{U}_j$.

Nach Lemma 5.15 ist die Anzahl n_i der Teilnehmer mit $l(P) \leq l_i$ gleich der Summe aus

- der Schwelle und
- dem Überhang des Levels l_i sowie
- den Überhängen aller höherwertigen Level.

Die folgende Definition dient erneut der einfacheren Formulierung der nachfolgenden Sätze.

5.16 Definition: MENGE DER MINIMALEN TEILNEHMER

Sei $G \in \Gamma$ eine zulässige Teilnehmermenge eines Multilevel Schemes und $M = M_1, M_2, \ldots, M_m$ die Minimalstruktur von G. Dann ist

$$M_G = \left\{ P \in G \,\middle|\, P \in M_i \text{ für ein } i = 1, 2, \ldots, m \right\}$$

definiert als die *Menge der minimalen Teilnehmer von G*.

Ein Teilnehmer gehört genau dann zur Menge der minimalen Teilnehmer von G, wenn er in mindestens einer minimalen Menge von G vorkommt.

In Teil III des Konsistenztestes aus Definition 5.4 werden alle Mengen $G' := G \setminus X$ (mit $X \subseteq G$) sukzessive (d.h. für wachsende $|X|$) daraufhin überprüft, ob sich die Mengen der minimalen Teilnehmer von G und G' unterscheiden. Die beiden folgenden Sätze klären, unter welchen Voraussetzungen Teilnehmer, die in einer minimalen Menge von G enthalten sind, in den minimalen Mengen von G' fehlen.

5.17 Satz:

Sei $G \in \Gamma$ eine zulässige Teilnehmermenge eines Multilevel Schemes. Sei ferner

$$G' := G \setminus X \text{ mit } X \subseteq G \text{ und } |X| < \ddot{U}_i + \ddot{U}_{i+1} + \ldots + \ddot{U}_{max}.$$

Dann gilt für alle Teilnehmer P mit $l(P) \leq l_i$:

$$P \in M_{G'}$$

$M_{G'}$ ist nach Definition 5.16 die Menge der minimalen Teilnehmer von G'.

Beweis:
Gezeigt wird:

a) Wenn X nicht mindestens $\ddot{U}_{max}$ Teilnehmer aus l_{max} enthält, dann ist l_{max} ein prüfbares Level von G'. Dann wäre l_{max} nach Definition 5.6 das Maximumlevel von G' und die Aussage des Satzes würde nach Satz 5.8 folgen.

b) Wenn X mindestens $\ddot{U}_{max}$ Teilnehmer aus l_{max}, jedoch nicht mindestens $\ddot{U}_{i_{max}-1}$ Teilnehmer aus $l_{i_{max}-1}$ enthält, ist $l_{i_{max}-1}$ ein prüfbares Level in G' und die Aussage des Satzes wäre richtig.

c) Aus a) und b) folgt die Aussage des Satzes.

Zu a)
Wenn l_{max} ein prüfbares Level in G' wäre, dann würde nach den Definitionen 5.5 und 5.13 gelten:

i) $n'_{max} > l_{max}$ und
ii) $\ddot{U}'_{max} > 0$

Dabei ist $\ddot{U}'_{max}$ der minimale Überhang des Levels l_{max} in G' und n'_{max} die Anzahl der Teilnehmer P mit: $P \in G'$ und $l(P) \leq l_{max}$

Zu i):
Für die Teilnehmeranzahl n'_{max} gilt (i_{max} ist nach Definition 5.6 der Index des Maximumlevels):

$$n'_{max} \geq n_{max} - |X| \quad (G' := G \setminus X)$$

$$= l_{max} + \sum_{j=1}^{i_{max}} \ddot{U}_j - |X| \quad \text{Nach Lemma 5.15}$$

$$> l_{max} + \sum_{j=1}^{i_{max}} \ddot{U}_j - \sum_{j=i}^{i_{max}} \ddot{U}_j \quad \text{n.V. gilt: } |X| < \ddot{U}_i + \ddot{U}_{i+1} + \ldots + \ddot{U}_{max}$$

$$\geq l_{max} \quad \text{wg. } \sum_{j=i}^{i_{max}-1} \ddot{U}_j \leq \sum_{j=1}^{i_{max}-1} \ddot{U}_j$$

Zu ii):
Die Anzahl der Teilnehmer P mit $l(P) = l_{max}$ und $P \in X$ sei: x_{max}. Nach Voraussetzung a) gilt: $x_{max} < \ddot{U}_{max}$

Dann gilt

$$\ddot{U}'_{max} = (n'_{max} - n'_{i_{max}-1}) - (l_{max} - l_{i_{max}-1}) \quad \text{Nach Lemma 5.15}$$

$$\geq (n_{max} - n_{i_{max}-1} - x_{max}) - (l_{max} - l_{i_{max}-1}) \quad G' := G \setminus X \Rightarrow n'_{max} - n'_{i_{max}-1} = n_{max} - n_{i_{max}-1} - x_{max}$$

$$> (n_{max} - n_{i_{max}-1} - \ddot{U}_{max}) - (l_{max} - l_{i_{max}-1}) \quad \text{n.V. } x_{max} < \ddot{U}_{max}$$

$$= (n_{max} - n_{i_{max}-1} - [(n_{max} - n_{i_{max}-1}) - (l_{max} - l_{i_{max}-1})]) - (l_{max} - l_{i_{max}-1})$$

$$= 0$$

Insgesamt gilt nach i) und ii) für die Voraussetzung a) die Aussage des Satzes.

Zu b):
Analog zu a) ist zu zeigen, dass $l_{i_{max}-1}$ ein prüfbares Level in G' ist, d.h. es ist zu zeigen:

i) $n'_{i_{max}-1} > l_{i_{max}-1}$ und
ii) $\ddot{U}'_{i_{max}-1} > 0$

Zu i):
Es gilt:

$$n'_{i_{max}-1} \geq n_{i_{max}-1} - (|X| - \ddot{U}_{max}) = l_{i_{max}-1} + \sum_{j=1}^{i_{max}-1} \ddot{U}_j - (|X| - \ddot{U}_{max}) > l_{i_{max}-1} + \sum_{j=1}^{i_{max}-1} \ddot{U}_j - \sum_{j=i}^{i_{max}-1} \ddot{U}_j \geq l_{i_{max}-1}$$

(n.V. sind mindestens $\ddot{U}_{max}$ Teilnehmer in X aus l_{max})

Zu ii):
Ebenfalls analog zu a) gilt (hier mit der Voraussetzung $x_{i_{max}\text{-}1} < \ddot{U}_{i_{max}\text{-}1}$):

$$\begin{aligned}\ddot{U}'_{i_{max}\text{-}1} &= (n'_{i_{max}\text{-}1} - n'_{i_{max}\text{-}2}) - (l_{i_{max}\text{-}1} - l_{i_{max}\text{-}2}) \\ &\geq (n'_{i_{max}\text{-}1} - n'_{i_{max}\text{-}2} - x_{i_{max}\text{-}1}) - (l_{i_{max}\text{-}1} - l_{i_{max}\text{-}2}) \\ &> (n_{i_{max}\text{-}1} - n_{i_{max}\text{-}2} - \ddot{U}_{i_{max}\text{-}1}) - (l_{i_{max}\text{-}1} - l_{i_{max}\text{-}2}) \\ &= 0\end{aligned}$$

Insgesamt gilt nach i) und ii) auch für die Voraussetzung b) die Aussage des Satzes.

Zu c):
Die Argumentation aus a) und b) lässt sich für die Level $l_{i_{max}\text{-}2}$, $l_{i_{max}\text{-}3}$, …, l_i fortsetzten. Da $|X| < \ddot{U}_i + \ddot{U}_{i+1} + ... + \ddot{U}_{max}$ gilt, kann die Voraussetzung, dass X mindestens $\ddot{U}_j$ Teilnehmer aus l_j enthalten soll, nicht für alle Level l_{max}, $l_{i_{max}\text{-}1}$, …, l_i erfüllt werden und das Maximumlevel von G' ist mindestens gleich l_i.

Daraus folgt nach Satz 5.8, dass jeder Teilnehmer P mit $l(P) \leq l_i$ in mindestens einer minimalen Menge von G' vorkommt.

Satz 5.17 sagt in Bezug auf den erweiterten Test auf Konsistenz für Multilevel Schemes aus, dass in den Ergebnismengen zu den Prüfmengen einer Ordnung kleiner als $\ddot{U}_i + \ddot{U}_{i+1} + ... + \ddot{U}_{max}$ kein Teilnehmer mit $l(P) \leq l_i$ enthalten ist. Insbesondere sind alle Ergebnismengen zu den Prüfmengen einer Ordnung kleiner als $\ddot{U}_{max}$ leer.

Nachdem nun gezeigt ist, dass Teilnehmer in den Ergebnismengen bis zu einer gewissen Ordnung der Prüfmengen *nicht* enthalten sind, klärt der folgende Satz, unter welchen Voraussetzungen sie in den Ergebnismengen höherer Ordnung vorkommen.

5.18 Satz:

Sei $G \in \Gamma$ eine zulässige Teilnehmermenge eines Multilevel Schemes. Sei ferner

$$G' := G \setminus X \text{ mit } X \subseteq G \text{ und } |X| = \ddot{U}_i + \ddot{U}_{i+1} + \ldots + \ddot{U}_{max}.$$

Schließlich sei $x_j := \left| \left\{ P \in X \;\middle|\; l(P) = l_j \right\} \right|$ (für $j = 1, 2, \ldots, t$).

a) Sei $x_j < \ddot{U}_j$ für (mindestens) ein $j \in \{i, i+1, \ldots, i_{max}\}$ $(i \geq 2)$.
Dann gilt für alle P mit $l(P) \leq l_i$: $P \in M_{G'}$

b) Sei $x_j = \ddot{U}_j$ für alle $j \in \{i, i+1, \ldots, i_{max}\}$. Dann gilt:
$P \notin M_{G'} \Leftrightarrow l(P) \geq l_i$ (für alle $P \in G'$ und $i \geq 2$)

$M_{G'}$ ist nach Definition 5.16 die Menge der minimalen Teilnehmer von G'.

Beweis:
Zu a):
Es gelte $x_j < \ddot{U}_j$ für (mindestens) ein $j \in \{i, i+1, \ldots, i_{max}\}$. Sei k das größte j, welches diese Voraussetzung erfüllt. Im folgenden wird gezeigt, dass l_k in G' ein prüfbares Level ist. Die Argumentation erfolgt analog zum Beweis von Satz 5.17.

Für die Anzahl n'_k der in G' enthaltenen Teilnehmer P mit $l(P) \le l_k$ gilt:

Da mindestens für diese Teilnehmer n.V. gilt: $l(P) > l_k$

$$n'_k \geq n_k - (|X| - \sum_{j=k+1}^{i_{max}} \ddot{U}_j)$$

Nach Lemma 5.15

$$= l_k + \sum_{j=1}^{k} \ddot{U}_j - (|X| - \sum_{j=k+1}^{i_{max}} \ddot{U}_j)$$

n.V. gilt: $|X| = \ddot{U}_i + \ddot{U}_{i+1} + \ldots + \ddot{U}_{max}$

$$= l_k + \sum_{j=1}^{k} \ddot{U}_j - \sum_{j=i}^{i_{max}} \ddot{U}_j + \sum_{j=k+1}^{i_{max}} \ddot{U}_j$$

Addition der 1. und 3. Summe

$$= l_k + \sum_{j=1}^{i_{max}} \ddot{U}_j - \sum_{j=i}^{i_{max}} \ddot{U}_j$$

n.V. gilt: $i \ge 2$; da l_1 prüfbar ist, gilt $\ddot{U}_1 > 0$

$$> l_k$$

In G' gilt folglich:

- $n'_k > l_k$ und
- $\ddot{U}_k > 0$ (folgt aus der Voraussetzung: $x_k < \ddot{U}_k$, Beweis analog zu Satz 5.17).

Daher ist l_k in G' ein prüfbares Level und nach Satz 5.8 folgt, dass ein Teilnehmer P mit $l(P) \le l_i \le l_k$ in mindestens einer minimalen Menge von G' vorkommt, also $P \in M_{G'}$.

Zu b):
Das Maximumlevel l'_{max} von G' ist gleich l_{i-1}, denn

i) mit einer zum Beweis von a) analogen Argumentation folgt: $n'_{i-1} > l_{i-1}$,

ii) ferner gilt nach Vereinbarung $\ddot{U}_{i-1} > 0$ (d.h. l_{i-1} ist ein prüfbares Level), und

iii) wegen $x_j = \ddot{U}_j$ für alle $j \in \{i, i+1, \ldots, i_{max}\}$ gilt in G': $\ddot{U}_j = 0$ für $j \ge i$ (d.h. l_{i-1} ist das größte prüfbare Level).

Da $l'_{max} = l_{i-1}$ gilt, sind nach Satz 5.8 in $M_{G'}$ genau alle Teilnehmer P mit $l(P) \le l_{i-1}$ enthalten.

Mit Hilfe der beiden letzten Sätze wird nunmehr gezeigt, dass in den Ergebnismengen E_{L}^{k} ($k = 1, \ldots, g$) des erweiterten Tests auf Konsistenz nach Definition 5.9 die Teilnehmer, nach ihren Levels sortiert, enthalten sind. Dabei werden die Sätze 5.17 und 5.18 folgendermaßen auf den Teil III des Tests angewendet:

Die in den beiden Sätzen jeweils betrachtete Menge $X = G \setminus G'$ entspricht den Prüfmengen G_k (vgl. Definitionen 4.7, 4.8 und Lemma 4.9). Die in Satz 5.18 b) notwendige Voraussetzung $x_j = \ddot{U}_j$ (mit $x_j = \left|\{P \in X \mid l(P) = l_j\}\right|$) entspricht folglich:

$$\left|\left\{P \in G_k \;\middle|\; l(P) = l_j\right\}\right| = \ddot{U}_j$$

Die Anzahl der Teilnehmer in X entspricht der Ordnung der Prüfmenge G_k.

Die Zusammensetzung der Ergebnismengen E_{L}^{k} lässt sich nach Definition 5.9 durch die folgenden Schritte bestimmen:

- Zunächst werden diejenigen Teilnehmer gesucht, die in keiner der minimalen Mengen zu $G \setminus G_k$ (d.h. in keiner der minimalen Mengen der Minimalstruktur $\underline{M}_k$) enthalten sind. Das sind zum einen die Teilnehmer aus G_k und zum anderen Teilnehmer aus Levels, die in $G \setminus G_k$ nicht prüfbar sind. (Zur Bestimmung dieser Teilnehmer können die Sätze 5.17 und 5.18 verwendet werden.)
- Die Restmengen R_i beinhalten
  - die Teilnehmer aus E_{N} und
  - diejenigen Teilnehmer, die in den Ergebnismengen E_{L}^{k} zu den Prüfmengen einer niedrigeren Ordnung als i enthalten (d.h. bereits einem Level zugeordnet) sind.
- Daraus können die Ergebnismengen E_k bestimmt werden. Sie enthalten alle Teilnehmer,
  - die in keiner minimalen Menge von $G \setminus G_k$ enthalten sind, außer denjenigen Teilnehmern,
  - die in einer Menge R_i einer niedrigeren Ordnung enthalten sind.
- Die E_{L}^{k} schließlich sind entweder leer (wenn die E_k keine Teilnehmer neben den Teilnehmern aus G_k enthalten), oder sie enthalten alle Teilnehmer aus E_k (wenn in der Minimalstruktur $\underline{M}_k$ neben den Teilnehmern aus G_k weitere Teilnehmer „fehlen“).

Im Beweis des folgenden Satzes werden wiederholt die obigen Schritte verwendet.

5.19 Satz:

Sei $G \in \Gamma$ eine zulässige Teilnehmermenge eines Multilevel Schemes. Der erweiterte Test auf Konsistenz werde nach Definition 5.9 durchgeführt. Der Test sei durchführbar (d.h. $E'^{\,0}_{\mathrm{M}} = \{\}$).

Betrachtet werden die Ergebnismengen E_L^k zu den Prüfmengen G_k der Ordnung $\ddot{U}_i + \ddot{U}_{i+1} + \ldots + \ddot{U}_{max}$, wobei für die Prüfmengen G_k gelte:

$$\left| \left\{ P \in G_k \mid l(P) = l_j \right\} \right| = \ddot{U}_j \text{ für } j = i, i+1, \ldots, i_{max}$$

Jede dieser Ergebnismengen E_L^k enthält genau alle Teilnehmer des Levels l_i. Alle anderen Ergebnismengen sind leer.

Beweis:
Der Beweis erfolgt durch vollständige Induktion nach der Ordnung der Prüfmengen. Gezeigt wird:

a) Der Satz gilt für die Ergebnismengen E_L^k zu Prüfmengen einer Ordnung kleiner gleich $\ddot{U}_{max}$.
b) Wenn der Satz für die Ergebnismengen E_L^k zu Prüfmengen G_k einer Ordnung kleiner gleich $\ddot{U}_i + \ddot{U}_{i+1} + \ldots + \ddot{U}_{max}$ gilt, dann gilt er auch für die Ergebnismengen zu Prüfmengen der Ordnung kleiner gleich $\ddot{U}_{i-1} + \ddot{U}_i + \ddot{U}_{i+1} + \ldots + \ddot{U}_{max}$ (für $i \geq 2$).

Zu a):

Nach Satz 5.17 sind alle Ergebnismengen zu den Prüfmengen einer Ordnung kleiner als $\ddot{U}_{max}$ leer und die Aussage des Satzes gilt.

Betrachtet werden nun Ergebnismengen E_L^k zu den Prüfmengen G_k der Ordnung gleich $\ddot{U}_{max}$. Dabei werden zwei Fälle unterschieden:

i) Sei $\left|\{P \in G_k \mid l(P) = l_{max}\}\right| = \ddot{U}_{max}$, d.h. jeder in den Prüfmengen G_k enthaltene Teilnehmer stamme aus dem Level l_{max}.

Dann sind nach Satz 5.18 in den zu den Prüfmengen G_k gehörenden Prüfstrukturen $\underline{M}_k$ (Definition 4.8) keine Teilnehmer des Levels l_{max} und keine Teilnehmer aus G_k enthalten. Nach Definition 5.9 folgt, dass in der Vereinigung der zugehörigen Ergebnismengen E_k genau alle Teilnehmer des Levels l_{max} enthalten sind. Da jeweils $E_k \supset G_k$ gilt, (denn es gibt in G mehr als $\ddot{U}_{max}$ Teilnehmer des Levels l_{max},) enthalten die zugehörigen Mengen E_L^k ebenfalls genau alle Teilnehmer des Levels l_{max}.

ii) Sei $\left|\{P \in G_k \mid l(P) = l_{max}\}\right| < \ddot{U}_{max}$, d.h. mindestens ein Teilnehmer der Prüfmengen G_k stamme nicht aus dem Level l_{max}.

Dann sind nach Satz 5.18 in den zu den Prüfmengen G_k gehörenden Prüfstrukturen $\underline{M}_k$ genau alle Teilnehmer P aus $G \setminus G_k$ mit $l(P) \leq l_{max}$ enthalten. Für die Teilnehmer P mit $l(P) > l_{max}$ gilt $P \in E_N = R_1$ (Satz 5.10 und Definition 5.9). Für die zugehörigen Ergebnismengen E_k gilt nach Definition 5.9:

$$\begin{aligned} E_k &= \left\{ P \in G \middle| P \notin M \text{ für alle } M \in \underline{M}_k \right\} \setminus R_{\ddot{U}_{max}} \\ &= \left(G_k \cup E_N \right) \setminus R_{\ddot{U}_{max}} \\ &= G_k \end{aligned}$$

Das bedeutet wiederum nach Definition 5.9: $E_L^k = \{\}$

Zu b):
Wenn der Satz für die Ergebnismengen E_L^k zu Prüfmengen einer Ordnung kleiner gleich $\ddot{U}_i + \ddot{U}_{i+1} + \ldots + \ddot{U}_{max}$ gilt, dann sind alle Teilnehmer der Levels $l_i, l_{i+1}, \ldots, l_{max}$ in diesen Ergebnismengen enthalten. Nach Definition 5.9 sind diese Teilnehmer daher in den Mengen R_O mit $O \leq \ddot{U}_i + \ddot{U}_{i+1} + \ldots + \ddot{U}_{max}$ (O sei die Ordnung der Prüfmengen) enthalten.

Zunächst werden alle Ergebnismengen E_L^k zu den Prüfmengen einer Ordnung O mit $\ddot{U}_{i-1} + \ddot{U}_i + \ddot{U}_{i+1} + \ldots + \ddot{U}_{max} > O > \ddot{U}_i + \ddot{U}_{i+1} + \ldots + \ddot{U}_{max}$ betrachtet. In den zugehörigen Prüfstrukturen $\underline{M}_k$ (Definition 4.8) sind nach Satz 5.17 (mindestens) alle Teilnehmer P aus $G \setminus G_k$ mit $l(P) \leq l_{i-1}$ enthalten. Für die Teilnehmer P mit $l(P) > l_{i-1}$ gilt nach obigen Überlegungen $P \in R_O$. Daher gilt nach Definition 5.9 für die zugehörigen Ergebnismengen: $E_k \subseteq G_k$ und folglich $E_L^k = \{\}$.

Betrachtet werden nun die Ergebnismengen E_L^k zu Prüfmengen der Ordnung $O = \ddot{U}_{i-1} + \ddot{U}_i + \ddot{U}_{i+1} + \ldots + \ddot{U}_{max}$. Dabei werden zwei Fälle unterschieden:

i) Sei $\left|\{P \in G_k \mid l(P) = l_j\}\right| = \ddot{U}_j$ für $j = i\text{-}1, i, i\text{+}1, \ldots, i_{max}$.

Nach Satz 5.18 sind in den zu den Prüfmengen G_k gehörenden Prüfstrukturen $\underline{M}_k$ (Definition 4.8) keine Teilnehmer des Levels l_{i-1} und keine Teilnehmer aus den Prüfmengen G_k enthalten. In G_k sind nach der Voraussetzung i) nur Teilnehmer enthalten, deren Level größer gleich l_{i-1} sind. Ferner sind nach den obigen Überlegungen alle Teilnehmer der Level größer gleich l_i bereits in den Mengen R_O enthalten. Daraus folgt nach Definition 5.9, dass die Vereinigung der zu den G_k gehörenden Ergebnismengen E_k genau alle Teilnehmer des Levels l_{i-1} enthalten.

Da $E_k \supset G_k$ gilt, (denn es gibt in G mehr als $\ddot{U}_{i-1}$ Teilnehmer des Levels l_{i-1},) enthalten die zugehörigen Mengen E_L^k ebenfalls genau alle Teilnehmer des Levels l_{i-1}.

ii) Sei $\left|\{P \in G_k \mid l(P) = l_j\}\right| < \ddot{U}_j$ für mindestens ein $j = i\text{-}1, i, i\text{+}1, \ldots, i_{max}$.

Dann sind nach Satz 5.18 in den zu den Prüfmengen G_k gehörenden Prüfstrukturen $\underline{M}_k$ (mindestens) alle Teilnehmer P aus $G \setminus G_k$ mit $l(P) \leq l_{i-1}$ enthalten. Für die Teilnehmer P mit $l(P) > l_{i-1}$ gilt $P \in R_O$. Für die zugehörigen Ergebnismengen E_k gilt nach Definition 5.9: $E_k \subseteq G_k$ und folglich $E_L^k = \{\}$.

Insgesamt ist also bewiesen, dass durch den erweiterten Test auf Konsistenz für Multilevel Schemes die Teilnehmer nach ihren Levels sortiert werden können. Die Ergebnismengen E_L^k sind entweder leer oder sie enthalten genau alle Teilnehmer eines Levels. Jedes Level ist in mindestens einer Ergebnismenge E_L^k enthalten.

Der Verlauf des erweiterten Test auf Konsistenz wird der folgenden Darstellung wiedergegeben.

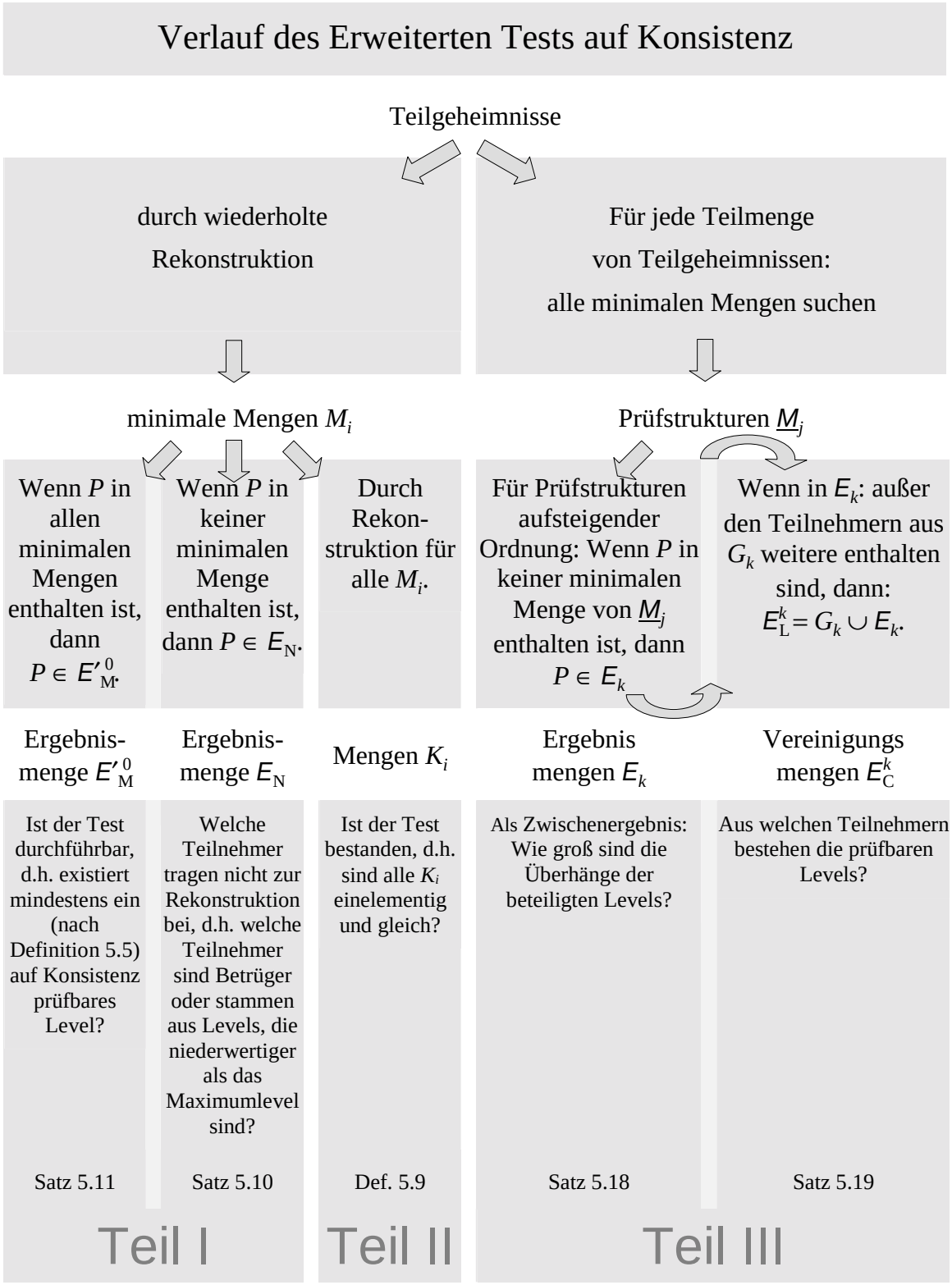


Abbildung 26: Verlauf des erweiterten Tests auf Konsistenz nach Definition 5.9

5.2.3 Sicherheitsaussagen für den erweiterten Test auf Konsistenz in der geometrischen Realisierung

Der erweiterte Test auf Konsistenz ist in der Lage, die Teilnehmer nach ihrer Zugehörigkeit zu den Levels zu sortieren. Es bleibt die Frage zu klären, mit welcher Wahrscheinlichkeit eine Zugriffskontrollinstanz einen Betrug oder einen Betrüger mit Hilfe des Testes entdecken kann.

Diese Frage kann (wie schon bei den Sicherheitsaussagen zu den Compartment Schemes ausgeführt) nur dann beantwortet werden, wenn eine konkrete Realisierung betrachtet wird. Für die folgenden Sicherheitsaussagen wird ein geometrisches Multilevel Scheme nach Definition 5.1 vorausgesetzt.

5.2.3.1 Prüfbare Teilnehmermengen

Die Sätze der nun folgenden Abschnitte haben eine gemeinsame Voraussetzung. Diese Voraussetzung wird in Definition 5.20 formuliert.

5.20 Definition: PRÜFBARE TEILNEHMERMENGEN EINES MULTILEVEL SCHEMES

Sei $G \in \Gamma$ eine zulässige Teilnehmermenge eines Multilevel Schemes nach Definition 2.7. Ferner sei P^i die Menge der Teilnehmer P, für die der Test $l(P) \leq l_i$ ermittelt. Schließlich sei x_i die Anzahl der Betrüger in P^i. Wenn für mindestens ein Level

$$x_i < l_i$$

gilt, dann heißt *G prüfbare Teilnehmermenge*.

Anmerkung:
Nach Vereinbarung sind alle an der Rekonstruktion beteiligten Levels im Sinne der Definition 5.5 prüfbar (vgl. S. 116). Ferner ist nach Satz 5.8 jeder Teilnehmer eines prüfbaren Levels in mindestens einer minimalen Menge enthalten. Wenn also für mindestens ein Level $x_i < l_i$ gilt, dann ist gewährleistet, dass mindestens ein ehrlicher Teilnehmer durch den erweiterten Test nach Definition 5.9 mit den anderen Teilnehmern auf Konsistenz geprüft wird.

5.2.3.2 Integrität des rekonstruierten Ergebnisses

Zunächst wird die Frage untersucht, wie hoch die Wahrscheinlichkeit dafür ist, dass die Teilnehmer tatsächlich K_0 und nicht einen anderen Schnittpunkt $K_x \neq K_0$ mit der Geheimnisgeraden rekonstruieren, wenn der Test auf Konsistenz bestanden wurde.

5.21 Satz:

Sei $G \in \Gamma$ eine nach Definition 5.20 prüfbare Teilnehmermenge eines geometrisch realisierten Multilevel Schemes, K_0 sei das verschlüsselte Geheimnis. Der erweiterte Test

auf Konsistenz werde nach Definition 5.9 durchgeführt. Der Test sei durchführbar und werde bestanden.

Dann ist das rekonstruierte Geheimnis mit der Wahrscheinlichkeit

$$p \geq p_E(l_{max})$$

gleich K_0. p_E ist die in Definition 3.15 eingeführte Erfolgswahrscheinlichkeit des erweiterten Tests auf Konsistenz.

Beweis:
Der Test ist nach Voraussetzung durchführbar und wird bestanden. Daraus folgt nach Definition 5.9: $E_M^0 = \{\}$. Nach Satz 5.11 muss daher für mindestens ein Level l_i gelten:

$$n_i > l_i$$

Da der Test auf Konsistenz bestanden wird, dürfen die mindestens l_i+1 Teilnehmer diese Levels l_i maximal einen (l_i-1)-dimensionalen Raum aufspannen. Die Wahrscheinlichkeit für diese Situation ist bei Anwesenheit von Betrügern nach Satz 3.14 kleiner gleich $1-p_E(l_i)$. Da l_{max} nach Definition 5.6 das größte prüfbare Level ist, gilt $p \geq p_E(l_{max})$.

5.2.3.3 Anwesenheit von Betrügern bei dem Test

Der nächste Satz gibt die Wahrscheinlichkeit dafür an, dass ein Betrüger bei Durchführung des erweiterten Tests auf Konsistenz nach Definition 5.9 in der Ergebnismenge E_N enthalten ist. Nach Satz 5.10 sind in E_N genau diejenigen Teilnehmer enthalten, die nicht zur Rekonstruktion beitragen. Gesucht ist also die Wahrscheinlichkeit, dass ein Betrüger nicht zur Rekonstruktion beiträgt (und sie daher nicht beeinflusst).

5.22 Satz:

Sei $G \in \Gamma$ eine nach Definition 5.20 prüfbare Teilnehmermenge eines geometrisch realisierten Multilevel Schemes. Der erweiterte Test auf Konsistenz werde nach Definition 5.9 durchgeführt. Der Test sei durchführbar (d.h. $E_M^0 = \{\}$).

Dann ist ein Betrüger mit der Wahrscheinlichkeit

$$p \geq 1 - \frac{q^{d-1} + q^{d-2} + \ldots + q - 1}{q^d + q^{d-1} + \ldots + q^2 - 1}$$

in der Menge E_N enthalten.

Beweis:
Ein Betrüger ist nach Definition 5.9 genau dann in E_N enthalten, wenn er nicht im Erzeugnis der ehrlichen, an der Rekonstruktion beteiligten Teilnehmer liegt.

Nach Definition 3.1 wird ein geometrisches Secret Sharing Scheme in PG(d, q), einem projektiven Raum der Dimension d realisiert. Für Multilevel Schemes gilt nach Definition 5.1 $d = l_t - 1 + s$. Ferner gilt nach Definition 5.1 für die Dimension d' des Erzeugnisses der ehrlichen Teilnehmer:

$$d' \leq l_t - 1 = d - s.$$

Folglich liegen in dem Erzeugnis der ehrlichen Teilnehmer höchstens (für $s = 1$) $q^{d-1} + q^{d-2} + \ldots + q + 1$ Punkte, von denen der Schnittpunkt des Erzeugnisses mit der Geheimnisgeraden sowie das Teilgeheimnis des Betrügers abgezogen werden.

Ein Betrüger hat a priori alle Punkte aus PG(d, q) zur Auswahl. Sein eigener und die Punkte der Geheimnisgeraden kommen für die Auswahl nicht in Frage, es bleiben also $q^d + q^{d-1} + \ldots + q^2 - 1$ Punkte.

Demnach gilt für die Wahrscheinlichkeit, dass ein Betrüger, der zufällig einen Punkt aus PG(d, q) wählt, in E_N enthalten ist:

$$p \geq 1 - \frac{q^{d-1} + q^{d-2} + \ldots + q - 1}{q^d + q^{d-1} + \ldots + q^2 - 1}$$

Der Satz lässt folgenden wichtigen Schluss zu:

Wenn $E_N = \{\}$, dann sind mit der angegebenen Wahrscheinlichkeit p alle Teilnehmer ehrlich.

Die andere Richtung der Aussage, nämlich von $E_N \neq \{\}$ auf das Vorhandensein eines oder mehrerer Betrüger zu schließen, ist im allgemeinen nicht richtig. In E_N sind nach Satz 5.10 auch diejenigen *ehrlichen* Teilnehmer enthalten, die nicht zur Rekonstruktion beitragen, weil sie aus Levels stammen, die in der betrachteten Teilnehmermenge nicht mit hinreichend vielen Teilnehmern vertreten sind.

5.2.3.4 Sicherheitsaussagen für die gefundenen Levels

Durch den erweiterten Test auf Konsistenz werden die Teilnehmer, die an der Rekonstruktion beteiligt sind, nach ihrer Zugehörigkeit zu den Levels sortiert. In Abschnitt 5.2.3.3 wurde bereits die Wahrscheinlichkeit dafür ermittelt, dass ein Betrüger in der Menge E_N enthalten ist. Im folgenden wird darüber hinaus noch die Frage beantwortet, wie hoch die Wahrscheinlichkeit dafür ist, dass in einem durch den Test rekonstruierten Level kein Betrüger enthalten ist.

5.23 Satz:

Sei $G \in \Gamma$ eine nach Definition 5.20 prüfbare Teilnehmermenge eines geometrisch nach Definition 5.1 in PG(d, q) realisierten Multilevel Schemes. Der erweiterte Test auf

Konsistenz werde nach Definition 5.9 durchgeführt. Der Test sei durchführbar (d.h. $E_M^0 = \{\}$).

Der Test rekonstruiere für das Level l_i:

$$n_i = l_i + v \text{ mit } v \geq 1.$$

Dann ist mit der Wahrscheinlichkeit

$$p \geq 1 - \binom{|G|}{l_i + v} \left(\frac{q^{l_i-1} + q^{l_i-2} + \ldots + q}{q^d + q^{d-1} + \ldots + q^2 + 2} \right)^v$$

kein Betrüger in l_i enthalten.

Beweis:
Der Beweis erfolgt analog zum Beweis zu Satz 4.24. Die einzelnen Beweisschritte werden hier verkürzt dargestellt.

Aus $n_i = l_i + v$ folgt nach Definition 5.1, dass $l_i + v$ Punkte in einem (l_i-1)-dimensionalen Raum liegen, der genau einen Schnittpunkt mit B_0 hat. Gesucht wird zunächst die Wahrscheinlichkeit dafür, dass unter diesen ($l_i + v$) Teilnehmern Betrüger sind.

Die Anzahl der ($l_i + v$)-elementigen Untermengen von G ist

$$n := \binom{|G|}{l_i + v}.$$

Seien $X_1, X_2, X_3, \ldots, X_{l_i+v}$ die Teilgeheimnispunkte der $l_i + v$ Teilnehmer. Sie müssen in einem (l_i-1)-dimensionalen Raum durch B_0 liegen. Die Wahrscheinlichkeit p^* dafür ist (s. Satz 4.24):

$$p^* \leq \left(\frac{q^{l_i-1} + q^{l_i-2} + \ldots + q}{q^d + q^{d-1} + \ldots + q^2 + 2} \right)^v$$

Für die Wahrscheinlichkeit p' eines erfolgreichen Betruges gilt:

$$p' \leq np^*$$

und insgesamt folgt

$$p \geq 1 - p' = 1 - np^* = 1 - \binom{|G|}{l_i + v} p^*$$

Anmerkungen:
Je mehr Teilnehmer innerhalb eines Levels an der Rekonstruktion teilnehmen (d.h. je größer v ist), desto geringer die Wahrscheinlichkeit, dass ein Betrüger unter den Teilnehmern ist.

Nach Satz 5.23 gilt für die Wahrscheinlichkeit eines erfolgreichen Betruges:

$$p' \leq \binom{|G|}{l_i + v} \left(\frac{q^{l_i-1} + q^{l_i-2} + \ldots + q}{q^d + q^{d-1} + \ldots + q^2 + 2} \right)^v$$

Nach Definition 5.1 gilt für die Dimension d des projektiven Raumes, in dem ein Multilevel Scheme realisiert wird:

$$d := l_t - 1 + s$$

Daraus folgt die Abschätzung $d \geq l_t$ (wobei das Gleichheitszeichen für $s = 1$ gilt). Daraus wiederum folgt:

$$\lim_{q \to \infty} p' = 0 \text{ (für } v \geq 1).$$

Die mit den letzten Sätzen abgeleiteten Aussagen des Testes sind in der nächsten Abbildung zusammengefasst.

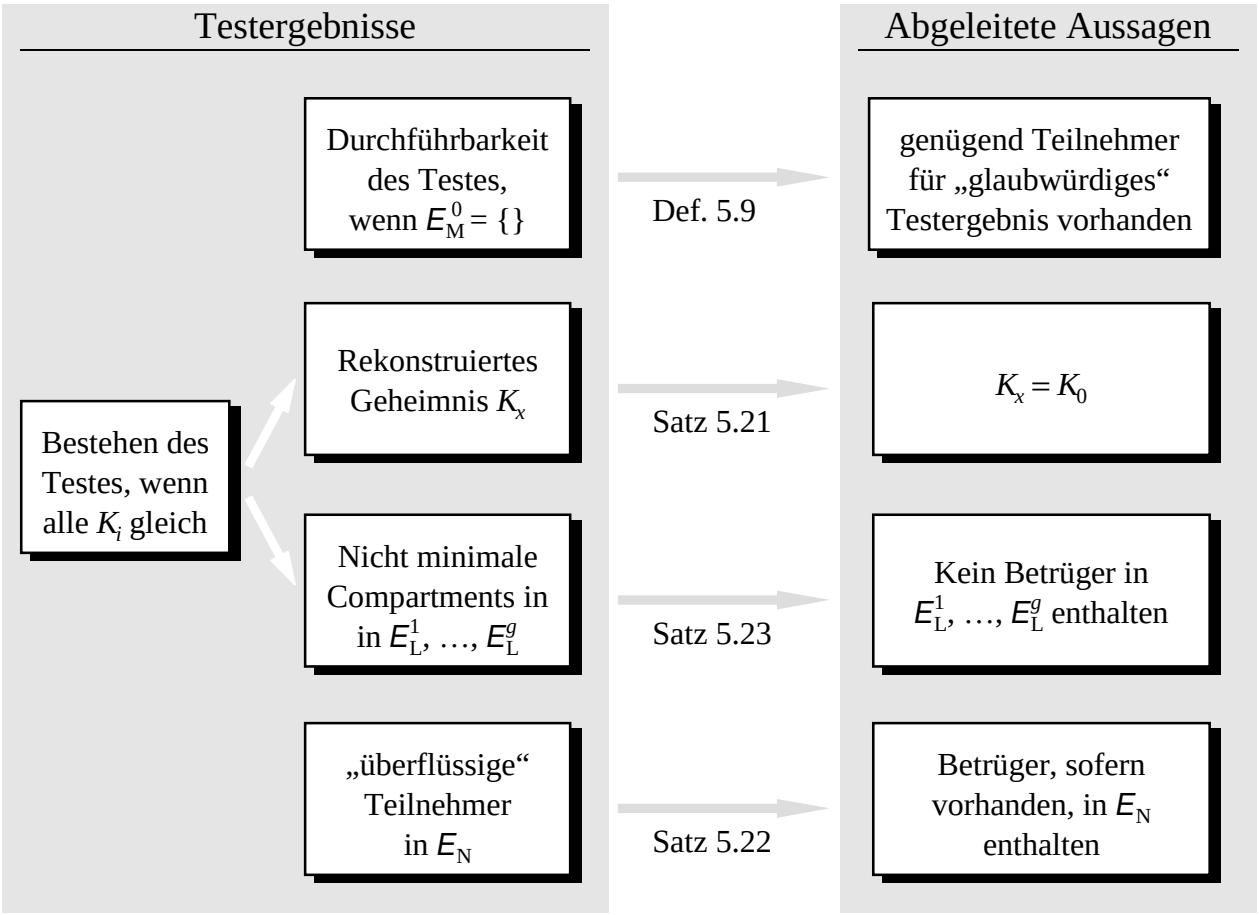


Abbildung 27: Aussagen des erweiterten Tests auf Konsistenz

5.3 Beispiel

Im folgenden wird der erweiterte Test auf Konsistenz für Multilevel Schemes an einem Beispiel durchgeführt. Ein (2, 3, 5)-Multilevel Scheme sei geometrisch realisiert. Die Teilnehmer $P_1, P_2, \ldots, P_6$ seien ehrlich, P_7 und P_8 seien Betrüger. Ihre Teilgeheimnispunkte liegen mit dem Punkt von P_5 auf einer Geraden. Die Situation ist in der Abbildung dargestellt.

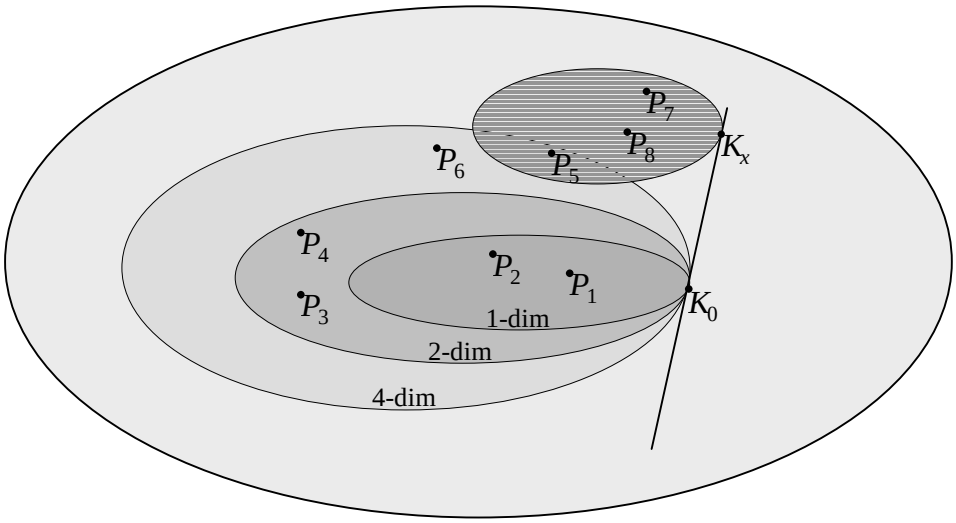


Abbildung 28: Ein (2, 3, 5)-Multilevel Scheme mit zwei Betrügern

In den nächsten Abschnitten wird für verschiedene Teilnehmermengen der Verlauf des erweiterten Testes auf Konsistenz beschrieben.

5.3.1 Test wird bestanden

Gegeben sei die Teilnehmermenge

$$G = \{P_1, P_2, P_3, P_4, P_7\}.$$

Nach Definition 2.11 ergeben sich die folgenden drei minimalen Mengen:

$$M_1 = \{P_1, P_2\},\ M_2 = \{P_1, P_3, P_4\},\ M_3 = \{P_2, P_3, P_4\}$$

Für die in Teil I des Tests berechneten Mengen gilt:

$$E'^{0}_{\mathrm{M}} := \{\, P \in G \mid P \in M_i \text{ für } \textit{alle } i = 1, 2, \ldots, m\} = \{\}$$
$$E_{\mathrm{N}} := \{\, P \in G \mid P \notin M_i \text{ für } \textit{alle } i = 1, 2, \ldots, m\} = \{P_7\}$$

Der Test ist demnach durchführbar ($E'^{0}_{\mathrm{M}} = \{\}$), über die Ehrlichkeit des Teilnehmers P_7 kann keine Aussage gemacht werden ($E_{\mathrm{N}} = \{P_7\}$).

In Teil II des Tests wird für alle minimalen Mengen die Rekonstruktion durchgeführt. Sei K_i das Rekonstruktionsergebnis der minimalen Menge M_i, dann gilt:

$$K_1 = K_2 = K_3 \ (= K_0)$$

Der Test wird bestanden.

Die folgende Tabelle gibt die Ergebnisse des Teil III des Test wieder. Die Spalte 2 der Tabelle enthält alle ein- und zweielementigen Teilmengen G_i von $G \setminus E_N$. Nach Definition 4.7 werden für diese Mengen G_i jeweils die Prüfstrukturen $\underline{M}_i$ gebildet ($\underline{M}_i$ enthält alle minimalen Mengen, deren Durchschnitt mit G_i leer ist). E_i enthält nach Definition 5.9 jeden Teilnehmer, der in keiner minimalen Mengen der Prüfmenge $\underline{M}_i$ vorkommt und nicht in R_k enthalten ist. Daraus werden schließlich die Mengen E_L^i gebildet, welche die Teilnehmer nach ihrer Zugehörigkeit zu den Levels sortieren:

i	G_i	$\underline{M}_i$	E_i	E_L^i	R_k
1	P_1	M_3	P_1	---	P_7
2	P_2	M_2	P_2	---	P_7
3	P_3	M_1	P_3, P_4	P_3, P_4	P_7
4	P_4	M_1	P_3, P_4	P_3, P_4	P_7
5	P_1, P_2	---	P_1, P_2	---	P_3, P_4, P_7
6	P_1, P_3	---	P_1, P_2	P_1, P_2	P_3, P_4, P_7
7	P_1, P_4	---	P_1, P_2	P_1, P_2	P_3, P_4, P_7
8	P_2, P_3	---	P_1, P_2	P_1, P_2	P_3, P_4, P_7
9	P_2, P_4	---	P_1, P_2	P_1, P_2	P_3, P_4, P_7
10	P_3, P_4	M_1	---	---	P_3, P_4, P_7

Die beiden beteiligten Level werden korrekt rekonstruiert. Teilnehmer P_7 bleibt zwar als Betrüger unerkannt, das Rekonstruktionsergebnis wird jedoch durch ihn nicht verfälscht.

5.3.2 Test wird nicht bestanden

Gegeben sei die Teilnehmermenge

$$G = \{P_1, P_2, P_5, P_7, P_8\}.$$

Zu dieser Teilnehmermenge existieren vier minimale Mengen:

$$M_1 = \{P_1, P_2\}$$
$$M_2 = \{P_5, P_7\}$$
$$M_3 = \{P_7, P_8\}$$
$$M_4 = \{P_5, P_8\}$$

Für die in Teil I des Tests berechneten Mengen gilt:

$$E'^0_M := \{ P \in G \mid P \in M_i \text{ für } \textit{alle } i = 1, 2, \ldots, m\} = \{\}$$
$$E_N := \{ P \in G \mid P \notin M_i \text{ für } \textit{alle } i = 1, 2, \ldots, m\} = \{\}$$

Der Test ist also nach Definition 5.9 durchführbar, da $E'^0_M = \{\}$.

In Teil II des Testes ergeben sich für die minimalen Mengen unterschiedliche Geheimnisse, der Test wird nicht bestanden:

$$K_0 = K_1 \neq K_2 = K_3 = K_4 = K_x$$

Die Betrüger sind in dieser Konstellation nicht in der Ergebnismenge E_N enthalten, da sie auf einer Geraden mit einem Punkt der Geheimnisgeraden und einem ehrlichen Teilnehmer liegen. Der Betrug wird jedoch entdeckt, der Test wird aufgrund der Gegenwart der Betrüger nicht bestanden.

5.3.3 Test ist nicht durchführbar

Gegeben sei die Teilnehmermenge

$$G = \{P_1, P_2, P_4, P_5, P_6\}.$$

Zu dieser Teilnehmermenge existiert eine minimale Menge:

$$M_1 = \{P_1, P_2\}$$

Für die in Teil I des Tests berechneten Mengen gilt:

$$E'^0_M := \{ P \in G \mid P \in M_i \text{ für } \textit{alle } i = 1, 2, \ldots, m\} = \{P_1, P_2\}$$
$$E_N := \{ P \in G \mid P \notin M_i \text{ für } \textit{alle } i = 1, 2, \ldots, m\} = \{\}$$

Der Test ist also nach Definition 5.9 nicht durchführbar, d.h. in der Teilnehmermenge G ist kein nach Definition 5.5 prüfbares Level enthalten.

5.3.4 Test rekonstruiert falsches Ergebnis

Gegeben sei die Teilnehmermenge

$$G = \{P_5, P_7, P_8\}.$$

Zu dieser Teilnehmermenge existieren drei minimalen Mengen:

$$M_1 = \{P_5, P_7\}$$
$$M_2 = \{P_7, P_8\}$$
$$M_3 = \{P_5, P_8\}$$

Für die in Teil I des Tests berechneten Mengen gilt:

$$E'^0_M := \{ P \in G \mid P \in M_i \text{ für } \textit{alle } i = 1, 2, \ldots, m\} = \{\}$$
$$E_N := \{ P \in G \mid P \notin M_i \text{ für } \textit{alle } i = 1, 2, \ldots, m\} = \{\}$$

Der Test ist nach Definition 5.9 durchführbar, da $E'^0_M = \{\}$.

Für alle minimalen Mengen wird dasselbe Geheimnis rekonstruiert. Es gilt

$$K_1 = K_2 = K_3 \ (= K_x)$$

Der Test wird also trotz der Gegenwart von Betrügern bestanden. Der ehrliche Teilnehmer P_5 würde dem falschen Geheimnis K_x trauen.

In Teil III des Testes werden die drei Teilnehmer demselben Level zugeordnet:

i	G_i	$\underline{M}_i$	E_i	E_L^i
1	P_5	M_2	P_5	---
2	P_7	M_3	P_7	---
3	P_8	M_1	P_8	---
4	P_5, P_7	---	P_5, P_7, P_8	P_5, P_7, P_8
5	P_5, P_8	---	P_5, P_7, P_8	P_5, P_7, P_8
6	P_7, P_8	---	P_5, P_7, P_8	P_5, P_7, P_8

5.4 Threshold Schemes als Spezialfall

Der erweiterte Test auf Konsistenz für Multilevel Schemes, wie er mit Definition 5.9 eingeführt wurde, ist gleichermaßen auf die Threshold Schemes anwendbar. Im folgenden wird gezeigt, dass es sich bei dem in Definition 3.12 eingeführten Test für Threshold Schemes um einen Spezialfall des hier behandelten Tests handelt.

Ein Threshold Scheme ist ein Multilevel Scheme nach Definition 2.7 mit $t = 1$, d.h. $\mathbb{L} = \{l_1\}$.

5.24 Satz:

Sei $G \in \Gamma$ eine zulässige Teilnehmermenge eines geometrisch nach Definition 3.2 in PG(d, q) realisierten Threshold Schemes. Die Tests auf Konsistenz werden nach den Definitionen 3.12 und 5.9 durchgeführt.

Dann gilt mit der Wahrscheinlichkeit $p_E(t)$:

$$D \neq \{\} \quad \Leftrightarrow \quad E'^0_M = \{\}$$

Beweis:
a) Zu zeigen: $D \neq \{\} \quad \Rightarrow \quad E'^0_M = \{\}$

Nach Definition 3.12 gilt:

$$D = \left\{ K \in \mathbb{K} \middle| K \in K_i, K_j \; (i \neq j) \right\}$$

D enthält demnach alle Elemente der Geheimnismenge $\mathbb{K}$, die von mindestens zwei minimalen Mengen von G rekonstruiert werden. Nach Satz 3.14 folgt daraus mit der Wahrscheinlichkeit $p_E(t)$, dass mindestens $t + 1$ ehrliche Teilnehmer in G enthalten sind. Daraus wiederum folgt, dass keiner der Teilnehmer in jeder minimalen Menge von G enthalten ist und somit gilt nach Definition 5.9:

$$E'^0_M = \{\}$$

b) Zu zeigen: $E'^{0}_{M} = \{\} \Rightarrow D \neq \{\}$

Nach Satz 5.11 folgt aus $E'^{0}_{M} = \{\}$:

$$n_i > l_i \text{ für mindestens ein } i = 1, \ldots, t.$$

Für das Threshold Scheme bedeutet das: Mindestens $t + 1$ Teilnehmer sind in G enthalten, die mit mindestens der Wahrscheinlichkeit p_E ehrlich sind.

Daraus folgt nach Definition 3.12:

$$D \neq \{\}$$

Der obige Satz besagt, dass beide Tests unter denselben Voraussetzungen durchführbar sind.

5.25 Satz:

Sei $G \in \Gamma$ eine zulässige Teilnehmermenge eines geometrisch nach Definition 3.2 in PG(d, q) realisierten Threshold Schemes. Die Tests auf Konsistenz werden nach den Definitionen 3.12 und 5.9 durchgeführt.

Dann wird der Test auf Konsistenz nach Definition 3.12 genau dann bestanden, wenn auch der Test auf Konsistenz nach Definition 5.9 bestanden wird.

Beweis:
Die Aussage des Satzes folgt trivialerweise aus den in Bezug auf das Bestehen des Testes identischen Definitionen 3.12 und 5.9.

5.26 Satz:

Sei $G \in \Gamma$ eine zulässige Teilnehmermenge eines geometrisch nach Definition 3.2 in PG(d, q) realisierten Threshold Schemes. Die Tests auf Konsistenz werden nach den Definitionen 3.12 und 5.9 durchgeführt. Die Tests seien durchführbar, d.h. es gelte $D \neq \{\}$ bzw. $E'^{0}_{M} = \{\}$.

Dann gilt für die nach Definition 3.12 berechnete Menge E_B und die nach Definition 5.9 ermittelte Menge E_N mit der Wahrscheinlichkeit $p_E(t)$:

$$E_B = E_N$$

Beweis:
a) $P \in E_B \Rightarrow P \in E_N$

Nach Satz 3.16 sind in E_B mit der Wahrscheinlichkeit $p_E(t)$ genau alle Betrüger im Sinne von Definition 2.13 enthalten. Das bedeutet für geometrische Threshold Schemes nach Definition 3.2, dass in E_B alle Teilnehmer enthalten sind, deren Teilgeheimnisse nicht im Indikatorblock B_0 liegen.

Ein Teilnehmer P, dessen Teilgeheimnis nicht in B_0 liegt, trägt nicht zur Rekonstruktion bei und ist daher in keiner minimalen Menge enthalten. Daher gilt nach Definition 5.9: $P \in E_N$

b) $P \in E_N \Rightarrow P \in E_B$

Aus $P \in E_N$ folgt, dass P in keiner minimalen Menge enthalten ist. Daraus folgt nach Definition 3.12 für den Test auf Konsistenz für Threshold Schemes: $P \notin E_E$, denn

$$E_E := \{ P \in G \mid \text{es existiert ein } i \text{ mit } P \in M_i \text{ und } K_i \in D\} \text{ und } P \notin M_i \text{ für alle } i.$$

Da nach Definition 3.12 ferner $E_B := G \setminus E_E$ gilt, folgt $P \in E_B$.

5.27 Satz:

Sei $G \in \Gamma$ eine zulässige Teilnehmermenge eines geometrisch nach Definition 3.2 in PG(d, q) realisierten Threshold Schemes. Die Tests auf Konsistenz werden nach den Definitionen 3.12 und 5.9 durchgeführt. Die Tests seien durchführbar, d.h. es gelte $D \neq \{\}$ bzw. $E'^0_M = \{\}$.

Dann gilt für die nach Definition 3.12 berechnete Menge E_E und die nach Definition 5.9 ermittelten Mengen $E_L^1, E_L^2, \ldots, E_L^g$ mit der Wahrscheinlichkeit $p_E(t)$:

$$E_E = E_L^1 \cup E_L^2 \cup \ldots \cup E_L^g$$

Beweis:
Nach Definition 3.12 gilt $E_B := G \setminus E_E$, daraus folgt $E_E := G \setminus E_B$. Ferner gilt nach Satz 5.26 $E_B = E_N$, d.h. $E_E = G \setminus E_N$

Es genügt also,

$$G \setminus E_N = E_L^1 \cup E_L^2 \cup \ldots \cup E_L^g$$

zu zeigen.

Nach Satz 5.10 sind in E_N genau die Teilnehmer enthalten, die nicht zur Rekonstruktion beitragen. In $G \setminus E_N$ sind folglich genau diejenigen Teilnehmer enthalten, die an der Rekonstruktion beteiligt sind.

Es bleibt also zu zeigen, dass auch in $E_L^1 \cup E_L^2 \cup \ldots \cup E_L^g$ alle Teilnehmer und nur Teilnehmer enthalten sind, die an der Rekonstruktion beteiligt sind. In dem Threshold Scheme gibt es nur ein Level, in dem alle Teilnehmer gleichberechtigt enthalten sind. Aus $E'^0_M = \{\}$ folgt nach Satz 5.11, dass das Level in G prüfbar ist, nach Definition 5.6 ist dieses Level das Maximumlevel l_{max} von G. Alle Teilnehmer mit $l(P) = l_{max}$ tragen zur Rekonstruktion bei, alle anderen nicht. Nach Satz 5.19 sind genau alle Teilnehmer dieses Levels in den Ergebnismengen E_L^k zu den Prüfmengen der Ordnung $\ddot{U}_{max}$ enthalten. Alle anderen Ergebnismengen sind leer.

Insgesamt gilt also $G \setminus E_N = E_L^1 \cup E_L^2 \cup \ldots \cup E_L^g$.

Insgesamt stellt der erweiterte Test auf Konsistenz für Threshold Schemes einen Spezialfall des Tests nach Definition 5.9 dar.

6. Abbildungsverzeichnis

7. Literaturverzeichnis

[ABDS96]	G. Atiniese, C. Blundo, A. De Santis, D.R. Stinson, *Constructions and Bounds for Visual Cryptography*, 23rd International Colloquium on Automata, Languages and Programming, Lecture Notes in Computer Science, Vol. 1099, 1996, 416-428
[Beu00]	A. Beutelspacher, *Geheimsprachen - Geschichte und Techniken*, 2. Auflage, Verlag C.H. Beck, 2000
[Beu01]	A. Beutelspacher, *Kryptologie*, 6. Auflage, Vieweg Verlag, 2001
[BK95]	A. Beutelspacher, A.G. Kersten, *Verteiltes Vertrauen durch geteilte Geheimnisse*, Mathematisches Institut, Universität Gießen, Bericht, 1995
[Bla79]	G.R. Blakley, *Safeguarding Cryptographic Keys*, Proceedings of the National Computer Conference, American Federation of Information Processing Societies, Vol. 48, 1979, 313-317
[BR01]	A. Beutelspacher, U. Rosenbaum, *Projektive Geometrie: Von den Grundlagen bis zur Anwendung*, 2. Auflage, Vieweg Verlag, 2001
[BS91]	E.F. Brickell, D.R. Stinson, *The Detection of Cheaters in Threshold Schemes*, SIAM Journal of Discrete Mathematics, Vol. 4, 1991, 502-510
[BSW01]	A. Beutelspacher, J. Schenk, K.D. Wolfenstetter, *Moderne Verfahren der Kryptographie – Von RSA zu Zero-Knowledge*, 4. Auflage, Vieweg Verlag, 2001
[Cac96]	C. Cachin, *On-Line Secret Sharing*, Cryptography and Coding V, Lecture Notes in Computer Science, Vol. 1025, 1996, 190-198
[Car95]	M. Carpentieri, *A Perfect Threshold Secret Sharing Scheme to Identify Cheaters*, Designs, Codes and Cryptography, Vol. 5, Kluwer Academic Publishers, 1995, 183-188
[CDV94]	M. Carpentieri, A. De Santis, U. Vaccaro, *Size of Shares and Probability of Cheating in Threshold Schemes*, Advances in Cryptology - EUROCRYPT, Lecture Notes in Computer Science, Vol. 765, 1994, 118-125

[CGMW97]	L. Chen, D. Gollmann, C.J. Mitchell, P. Wild, *Secret Sharing with Reusable Polynomials*, Information Security and Privacy - ACISP, Lecture Notes in Computer Science, Vol. 1270, 1997, 183-193
[Czi97]	L. Czirmaz, *The Size of a Share Must be Large*, Journal of Cryptology, Vol. 10, Springer, 1997, 223-231
[DH76]	W. Diffie, M.E. Hellman, *New directions in Cryptography*, IEEE Transactions on Information Theory, IT-22, Vol. 6, 1976, 644-654
[Fia97]	A. Fiat, *Batch RSA*, Journal of Cryptology, Vol. 10, Springer, 1997, 75-88
[Gol98]	J.D. Golic, *On Matroid Characterization of Ideal Secret Sharing Schemes*, Journal of Cryptology, Vol. 11, Springer, 1998, 75-86
[HC96]	S.J. Hwang, C.C. Chang, *A Dynamic Secret Sharing Scheme with Cheater Detection*, Information Security and Privacy, Lecture Notes in Computer Science, Vol. 1172, 1996, 48-55
[Ker92]	A. Kersten, *Shared Secret Schemes aus geometrischer Sicht*, Dissertation, Mitteilungen aus dem Mathematischen Seminar Gießen, 1992, 208ff
[Kle92]	T. Kleiber, *Sicherheitskonzepte bei Shared Secret Schemes*, Diplomarbeit, Gießen, 1992
[Luc97]	N. Luckhardt, *Zeichensetzung: c't startet Krypto-Kampagne*, c't Magazin für Computertechnik, Verlag Heinz Heise, 1997, Heft 4, 32
[MS81]	R.J. McEliece, D.V. Sarwate, *On Sharing Secrets and Reed-Solomon Codes*, Communications of the ACM, Vol. 24, 1981, 583-584
[NP97]	M. Naor, B. Pinkas, *Visual Authetication and Identification*, Advances in Cryptology - CRYPTO, Lecture Notes in Computer Science, Vol. 1294, 1997, 322-336
[NS95]	M. Naor, A. Shamir, *Visual Cryptography*, Advances in Cryptology – EUROCRYPT, Lecture Notes in Computer Science, Vol. 950, 1995, 1-12
[NS97]	M. Naor, A. Shamir, *Visual Cryptography II: Improving the Contrast via the Cover Base*, Security Protocols, Lecture Notes in Computer Science, Vol. 1189, 1997, 197-202

[Neh93]	R. Nehl, *Robuste Shared Secret Schemes*, Dissertation Gießen, 1993
[OK98]	W. Ogata, K. Kurosawa, *Some Basic Properties of General Nonperfect Secret Sharing Schemes*, Journal of Universal Computer Science, Vol. 4, Springer, 1998, 690-704
[RB89]	T. Rabin, M. Ben-Or, *Verifiable Secret Sharing and Multiparty Protocols with Honest Majority*, 21st Annual Symposium on Theory of Computing, ACM Press, 1989, 73-85
[RS97]	R.L. Rivest, A. Shamir, *PayWord and MicroMint: Two Simple Micro-payment Schemes*, Security Protocols, Lecture Notes in Computer Science, Vol. 1189, 1997, 69-88
[RSA78]	R.L. Rivest, A. Shamir, L. Adleman, *A Method For Obtaining Digital Signatures And Public-Key Cryptosystems*, Communications of the ACM, Vol. 21, 120-126
[Sch95]	C. Schulze, *Multifunktionale Shared Secret Schemes*, Dissertation, Gießen, 1995
[Sch98]	R. Scheidler, *A Public-Key Cryptosystem Using Purely Cubic Fields*, Journal of Cryptology, Vol. 11, Springer, 1998, 109-124
[Sch99]	B. Schoenmakers, *A Simple Publicly Verifiable Secret Sharing Scheme and Its Application to Electronic Voting*, Advances in Cryptology - CRYPTO, Lecture Notes in Computer Science, Vol. 1666, 1999, 148-164
[Sha79]	A. Shamir, *How to Share a Secret*, Communications of the ACM, Vol. 22, 1979, 612-613
[Sim89]	G.J. Simmons, *Robust Shared Secret Schemes or „How to be Sure You Have the Right Answer Even Though You Don't Know the Question"*, Congressus Numerantium, Vol. 68, 1989, 215-248
[Sim89]	G.J. Simmons, *How to (Really) Share a Secret*, Advances in Cryptology - CRYPTO, Lecture Notes in Computer Science, Vol. 403, 1989, 390-448
[Sim92]	G.J. Simmons, *An Introduction to Shared Secret And/Or Shared Control Schemes And Their Application*, Contemporary Cryptology: The Science of Information Integrity, IEEE Press 1992, 441-497

[Sta96]	M. Stadler, *Publicly Verifiable Secret Sharing*, Advances in Cryptology - EUROCRYPT, Lecture Notes in Computer Science, Vol. 1070, 1996, 190-199
[Sti92]	D.R. Stinson, *An Explication of Shared Secret Schemes*, Designs, Codes and Cryptography, Vol. 2, 1992, 357-390
[SW98]	D.R. Stinson, R. Wei, *Bibliography On Secret Sharing Schemes*, http://www.cacr.math.uwaterloo.ca/~dstinson/ssbib.html, Ver. 4.1, 1998
[SU97]	J.U. Schmidt, B. Ungerer, *Al dente – Die Diskussion um Kryptographie*, Multiuser Multitasking Magazin iX, Verlag Heinz Heise, 1997, Heft 4, 128-131
[TW88]	M. Tompa, H. Woll, *How to Share a Secret with Cheaters*, Journal of Cryptology, Vol. 1, Springer, 1988, 133-138
[YY01]	A. Young, M. Yung, *A PVSS as Hard as Discrete Log and Shareholder Separability*, Public Key Cryptography, Lecture Notes in Computer Science, Vol. 1992, 2001, 287-299