Digitale Unterschriften mittels birationaler Permutationen

Thorsten Theobald

Diplomarbeit
am Fachbereich Informatik der
Johann Wolfgang Goethe-Universität
Frankfurt am Main

Betreuer: Prof. Dr. C. P. Schnorr

Digitale Unterschriften mittels birationaler Permutationen

Zusammenfassung

Im Jahr 1993 schlug A. Shamir Protokolle zur Erstellung digitaler Unterschriften vor, die auf rationalen Funktionen kleinen Grades beruhen. D. Coppersmith, J. Stern und S. Vaudenay präsentierten die ersten Angriffe auf die Verfahren. Diese Angriffe können den geheimen Schlüssel nicht ermitteln. Für eine der von Shamir vorgeschlagenen Varianten zeigen wir, wie der geheime Schlüssel ermittelt werden kann.

Das zweite Signaturschema von Shamir hängt von der Wahl einer algebraischen Basis ab. Eine besondere Bedeutung haben Basen, deren Elemente polynomiale Terme vom Grad 2 sind. Wir analysieren die Struktur der algebraischen Basen. Für den hervorgehobenen Spezialfall kann eine vollständige Klassifikation durchgeführt werden.

Erklärung

Hiermit versichere ich, daß ich diese Arbeit selbständig verfaßt und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe.

Frankfurt am Main, den 3. Januar 1995

Danksagung

Bedanken möchte ich mich bei Herrn Prof. Dr. Claus Schnorr für die Betreuung der Diplomarbeit. Seine Vorschläge und Anregungen trugen wesentlich zum Gelingen dieser Arbeit bei. Für wertvolle Hinweise und Diskussionen danke ich Herrn Serge Vaudenay von der Ecole Normale Supérieure in Paris.

Inhaltsverzeichnis

Einleitung

Eine digitale Unterschrift zu einer elektronischen Nachricht soll zweifelsfrei nachweisen, wer der Urheber der übermittelten Information ist. Sie bildet das digitale Analogon zu einer handgeschriebenen Signatur.

Das starke Wachstum im Bereich der Telekommunikation hat dazu beigetragen, daß die Bedeutung von Authentikationsmechanismen in den letzten Jahren erheblich zugenommen hat. Ein wichtiger Meilenstein in dieser Entwicklung wurde 1991 gesetzt: Das National Institute of Standards and Technology (NIST) verkündete einen US-Standard für digitale Unterschriften. Die unterschiedlichen Reaktionen auf dieses Ereignis verdeutlichen jedoch, daß der eingeführte Standard noch längst nicht alle Wünsche befriedigt. Aus diesem Grund ist es unerläßlich, weitere Konzepte zu untersuchen und deren Sicherheit zu analysieren.

In der vorliegenden Arbeit betrachten wir Protokolle auf der Grundlage einer Klasse rationaler Abbildungen, sogenannten birationalen Permutationen. Dieser Ansatz wurde im Jahr 1993 von A. Shamir (1993b) vorgestellt. Die Verfahren erschienen sehr attraktiv, weil der benötigte Rechenaufwand niedrig ist. Unterschriften können mit wenigen modularen Multiplikationen generiert oder verifiziert werden. Das zweite Schema von Shamir hängt von der Wahl einer algebraischen Basis ab. Shamir schlägt zwei Basen vor: eine symmetrische und eine asymmetrische.

Wir geben nun eine Übersicht über den Inhalt dieser Arbeit. Im ersten Kapitel stellen wir die benötigten Begriffe aus dem Bereich der Public-key Kryptographie zusammen.

Die beiden nächsten Kapitel sind dem Schema der sequentiellen Linearisierung gewidmet. Zunächst wird das Verfahren erläutert und danach gezeigt, wie das Verfahren erfolgreich angegriffen werden kann.

In Kapitel 4 wird das Schema der algebraischen Basen vorgestellt. Coppersmith, Stern und Vaudenay (1993) skizzieren einen Angriff auf die symmetrische Basis. Der geheime Schlüssel wird dabei nicht gefunden. Die Ausführung dieser Ideen erfolgt in Kapitel 5. Im daran anschließenden Kapitel erläutern wir den Angriff auf die asymmetrische Basis. Wir zeigen, wie der geheime Schlüssel ermittelt werden kann. In Kapitel 7 wird der Angriff auf eine Basis vorgestellt, welche zu Entartungen in dem Signaturschema führt.

Das letzte Kapitel beschäftigt sich mit der Charakterisierung der algebraischen Basen.

Kapitel 1

Grundlagen

In diesem Kapitel werden die notwendigen Begriffe aus dem Gebiet der Public-key Kryptographie eingeführt. Eine ausführliche Darstellung findet sich im Buch von Schneier (1994), eine gute Übersicht in der Arbeit von Rivest (1990).

1.1 Public-key Kryptographie

Ausgangspunkt für die Einführung der Public-key Kryptographie durch Diffie und Hellman (1977) waren vor allem zwei Fragestellungen:

- Zwei Parteien möchten mit Hilfe kryptographischer Methoden miteinander kommunizieren, ohne dabei von anderen abgehört zu werden. Kann ein vorheriges Treffen der beiden Gruppen zur geheimen Vereinbarung der Codierschlüssel vermieden werden?

- Gibt es einen Mechanismus, der dem Empfänger einer rein elektronischen Nachricht zweifelsfrei bestätigt, wer der Urheber dieser Nachricht ist? Im Falle eines nicht-elektronischen Dokuments wird dieser Nachweis durch eine handgeschriebene Signatur geliefert.

Beide Probleme können durch die Konzepte der Einwegfunktionen und Trapdoor-Funktionen gelöst werden. Eine **Einwegfunktion** (one-way function) ist eine Funktion, die schnell zu berechnen ist, deren Umkehrung aber einen praktisch nicht durchführbaren Rechenaufwand erfordert. Eine **Trapdoor-Funktion** ist eine Einwegfunktion, die mit einer geheimen Zusatzinformation schnell invertiert werden kann.

In **Public-key Kryptosystemen** (**asymmetrischen Kryptosystemen**) besitzt jeder Teilnehmer eines Systems ein Schlüsselpaar, das aus einem **privaten Schlüssel** (private key) und einem **öffentlichen Schlüssel** (public key) besteht. Der öffentliche Schlüssel wird bekanntgegeben. Er beschreibt eine Einwegfunktion und dient zum Codieren der

Nachrichten. Der private Schlüssel wird dagegen geheimgehalten. Er bildet die Zusatzinformation, mit deren Hilfe die Einwegfunktion schnell invertiert werden kann, und wird zum Decodieren benutzt.

1.2 Digitale Unterschriften

Ein Mechanismus zur Erstellung digitaler Unterschriften muß mehrere Forderungen erfüllen:

- Jeder Teilnehmer eines Systems kann effizient Unterschriften generieren, die ihn als den Urheber einer Nachricht auszeichnen.
- Sowohl der Empfänger einer Mitteilung als auch unabhängige Dritte können mit geringem Aufwand die Unterschrift verifizieren.
- Es ist unmöglich, die Unterschrift eines anderen Benutzers zu erzeugen.

Das Problem wird durch die Methoden der Public-key Kryptographie wie folgt gelöst: Ein Teilnehmer A verwendet seinen geheimen Schlüssel, um eine Nachricht zu unterzeichnen. Mit dem öffentlich bekannten Schlüssel von A kann die Unterschrift verifiziert werden.

Eine Nachricht m kann eine beliebige Länge besitzen. Deshalb ist es praktischer und effizienter, nicht die Nachricht m selbst, sondern einen kurzen Repräsentanten von m zu signieren. Zu diesem Zweck wird m durch eine **kryptographische Hashfunktion** h vom Nachrichtenraum in einen kleineren Raum abgebildet. Das Auffinden zweier verschiedener Elemente x und y mit $h(x) = h(y)$, sogenannten **Kollisionen**, ist für eine kryptographische Hashfunktion so aufwendig, daß dies praktisch nicht durchführbar ist.

Codierverfahren müssen gewährleisten, daß das Dechiffrieren in eindeutiger Weise wieder den ursprünglichen Text liefert. Im Gegensatz dazu brauchen digitale Unterschriften nicht eindeutig zu sein. Es ist durchaus erlaubt, daß es für einige oder alle Nachrichten mehrere zulässige Unterschriften gibt. Dieser Unterschied bewirkt, daß es Einwegfunktionen gibt, die nur in Zusammenhang mit Signaturmechanismen geeignet sind. Einen solchen Kandidaten stellen Polynomgleichungen dar, die wir im folgenden untersuchen werden. Der Vorteil von Systemen, welche nicht-eindeutige Unterschriften generieren, liegt darin, daß sogenannte **Interpolationsangriffe** vermieden werden. Hinter diesem Begriff verbergen sich kryptographische Angriffe, bei denen mit Hilfe der Interpolation von bekannten Unterschriften versucht wird, andere Nachrichten zu unterzeichnen.

Kapitel 2

Unterschriften auf der Grundlage sequentieller Linearisierung

In diesem Kapitel wird das von SHAMIR (1993b) vorgeschlagene Schema der sequentiellen Linearisierung präsentiert.

2.1 Mathematische Hilfsmittel

Wegen der nicht-einheitlichen Terminologie auf dem Gebiet der multivariaten Polynomringe in der Literatur stellen wir hier einige wichtige Begriffe zusammen.

Sei R ein kommutativer Ring mit Einselement und $R[x_1, \ldots, x_k]$ der Polynomring in den Variablen $x_1, \ldots, x_k$ über R.

Ein **Term** in $x_1, \ldots, x_k$ ist ein Produkt der Form

$$x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_k^{\alpha_k}$$

mit nichtnegativen ganzen Zahlen $\alpha_1, \ldots, \alpha_k$. Der **totale Grad** des Terms ist die Summe $\alpha_1 + \ldots + \alpha_k$.

Ein **Monom** in $x_1, \ldots, x_k$ über R ist ein Produkt der Form

$$m = a \cdot t,$$

wobei $a \neq 0$ aus R und t ein Term in $x_1, \ldots, x_k$ ist.

Ein Polynom $f \in R[x_1, \ldots, x_k]$ heißt **homogen linear** bzw. **homogen quadratisch**, wenn jeder Term von f den totalen Grad 1 bzw. 2 hat. Ein homogen quadratisches Polynom wird auch als **homogene quadratische Form** bezeichnet.

Definition 2.1 Sei K ein Körper. Ein Gleichungssystem mit k Polynomgleichungen über K in den Variablen $x_1, \ldots, x_k$ heißt **sequentiell linearisiert**, wenn gilt:

1. Die i-te Gleichung des Systems hängt nur von den Variablen $x_1, \ldots, x_i$ ab.
2. In der i-ten Gleichung tritt x_i linear (d.h. vom Grad 1) auf, so daß die i-te Gleichung nach x_i auflösbar ist.

Die Polynome $p_1(x_1, \ldots, x_k), \ldots, p_k(x_1, \ldots, x_k)$ heißen **sequentiell linearisiert**, wenn das Gleichungssystem

$$p_1(x_1, \ldots, x_k) = 0, \ldots, p_k(x_1, \ldots, x_k) = 0$$

sequentiell linearisiert ist.

Ein sequentiell linearisiertes Gleichungssystem kann sukzessive nach $x_1, x_2, \ldots, x_k$ aufgelöst werden.

Im folgenden bezeichnet $K(x_1, \ldots, x_k)$ den Quotientenkörper von $K[x_1, \ldots, x_k]$. Unter einer birationalen Permutation versteht man eine rationale Funktion, deren Inverse ebenfalls rational ist:

Definition 2.2 Sei K ein endlicher Körper, $K_1, K_2 \subseteq K^k$. Das Paar (f, g) mit $f = (f_1, \ldots, f_k) \in K(x_1, \ldots, x_k)^k$, $g = (g_1, \ldots, g_k) \in K(y_1, \ldots, y_k)^k$ heißt eine **birationale Permutation von K^k bezüglich der Definitionsbereiche K_1 und K_2**, wenn gilt:

1. Für alle $x = (x_1, \ldots, x_k) \in K_1$ ist $g(f(x_1, \ldots, x_k))$ definiert, und es gilt
$$g(f(x_1, \ldots, x_k)) = (x_1, \ldots, x_k).$$
2. Für alle $y = (y_1, \ldots, y_k) \in K_2$ ist $f(g(y_1, \ldots, y_k))$ definiert, und es gilt
$$f(g(y_1, \ldots, y_k)) = (y_1, \ldots, y_k).$$

Bemerkung 2.3 Man ist an birationalen Permutationen interessiert, für die die Mengen $K^k \setminus K_1$ und $K^k \setminus K_2$ nur wenige Elemente enthalten.

2.2 Generieren eines Schlüsselpaares

Das Prinzip der sequentiellen Linearisierung wird verwendet, um ein einfach zu lösendes polynomiales Gleichungssystem zu generieren. Zwei lineare Transformationen verwandeln dieses System in ein anderes, welches wesentlich schwieriger zu lösen ist. Das Ausgangssystem und die beiden Transformationen bilden den privaten Schlüssel. Das transformierte System wird als öffentlicher Schlüssel bekanntgegeben. Lösungen des veröffentlichten Gleichungssystems stellen gültige Unterschriften dar.

Seien p und q große Primzahlen, $n := p \cdot q$. Die Faktorisierung des Moduls n sei den Benutzern des Systems nicht bekannt. Im folgenden werden alle Rechnungen im Ring der ganzen Zahlen modulo n durchgeführt. Wir betrachten die k Gleichungen

$$\begin{aligned} g_1 &= y_1 \pmod n, \\ g_2 &= y_1 y_2 \pmod n, \\ g_i &= l_i(y_1, \ldots, y_{i-1}) \cdot y_i + q_i(y_1, \ldots, y_{i-1}) \pmod n, \quad 3 \le i \le k. \end{aligned} \tag{2.1}$$

Dabei soll l_i ein homogenes lineares Polynom in $y_1, \ldots, y_{i-1}$ mit $l_i \neq 0$ sein, $3 \le i \le k$. Die Funktion q_i soll eine homogene quadratische Form in $y_1, \ldots, y_{i-1}$ sein, $3 \le i \le k$. Das beschriebene System ist sequentiell linearisiert. Für $2 \le i \le k$ ist g_i eine homogene quadratische Form in $y_1, \ldots, y_i$.

Variablentransformation: Eine zufällig gewählte invertierbare Matrix A beschreibt eine lineare Variablentransformation A von den **ursprünglichen Variablen** $y_1, \ldots, y_k$ zu den **neuen Variablen** $x_1, \ldots, x_k$.

$$\begin{pmatrix} y_1 \\ \vdots \\ y_k \end{pmatrix} = A \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix}$$

Linearkombinationen der Gleichungen: Mit Hilfe einer zufällig gewählten invertierbaren Matrix B werden die Gleichungen linear miteinander kombiniert.

$$\begin{pmatrix} f_1 \\ \vdots \\ f_k \end{pmatrix} = B \cdot \begin{pmatrix} g_1 \\ \vdots \\ g_k \end{pmatrix}$$

Beispiel 2.4 $k = 3$, $p = 31$, $q = 29$, $n = p \cdot q = 899$. Alle Gleichungen sind modulo 899 aufzufassen.

$$\begin{aligned} g_1 &= y_1 \\ g_2 &= y_1 y_2 \\ g_3 &= 782y_1^2 + 675y_1y_2 + 249y_2^2 + (112y_1 + 385y_2) \cdot y_3 \end{aligned}$$

$$A = \begin{pmatrix} 1 & 456 & 23 \\ 1 & 593 & 205 \\ 1 & 873 & 125 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 435 & 760 \\ 0 & 422 & 391 \end{pmatrix}.$$

Damit ergibt sich für $g_1, \ldots, g_k$ in den neuen Variablen

$$\begin{aligned} g_1 &= x_1 + 456x_2 + 23x_3 \\ g_2 &= x_1^2 + 150x_1x_2 + 708x_2^2 + 228x_1x_3 + 138x_2x_3 + 220x_3^2 \\ g_3 &= 405x_1^2 + 733x_1x_2 + 674x_2^2 + 472x_1x_3 + 829x_2x_3 + 325x_3^2 \end{aligned}$$

Die aus den Linearkombinationen hervorgehenden Gleichungen lauten

$$\begin{aligned} f_1 &= x_1 + 456x_2 + 23x_3 \\ f_2 &= 777x_1^2 + 222x_1x_2 + 332x_2^2 + 309x_1x_3 + 537x_2x_3 + 181x_3^2 \\ f_3 &= 553x_1^2 + 192x_1x_2 + 435x_2^2 + 280x_1x_3 + 300x_2x_3 + 559x_3^2 \end{aligned}$$

Um die Größe des privaten Schlüssels klein zu halten, sollen die Einträge in der ersten Spalte der Matrix A die Zahl 1 enthalten.

Um die Größe des öffentlichen Schlüssels klein zu halten, sollen die Polynome $f_2, \ldots, f_k$ homogene quadratische Formen in den Variablen $x_1, \ldots, x_k$ sein. Die erste Spalte von B soll deshalb $(1, 0, \ldots, 0)^T$ lauten.

Die Polynome $f_2, \ldots, f_k$ in den neuen Variablen werden veröffentlicht. Der Ausdruck für f_1 ist keine homogene quadratische Form. f_1 wird nicht bekanntgegeben.

2.3 Unterschreiben einer Nachricht

$h_2, \ldots, h_k$ seien öffentlich bekannte kryptographische Hashfunktionen mit Wertebereich $\mathbb{Z}_n$. Jeder Zahlenvektor $(x_1, \ldots, x_k) \in \mathbb{Z}_n^k$, der Lösung der $k-1$ Kongruenzen

$$f_i(x_1, \ldots, x_k) = h_i(m) \pmod{n}, \quad 2 \leq i \leq k,$$

ist, bildet eine gültige Unterschrift.

Um mit Hilfe des geheimen Schlüssels einen gültigen Vektor $(x_1, \ldots, x_k)$ zu ermitteln, wird zunächst ein zufälliger Wert für $f_1(x_1, \ldots, x_k)$ gewählt. Die Inverse der Matrix B wird verwendet, um mittels

$$\begin{pmatrix} g_1 \\ \vdots \\ g_k \end{pmatrix} = B^{-1} \cdot \begin{pmatrix} f_1 \\ \vdots \\ f_k \end{pmatrix}$$

die Werte für $g_1, \ldots, g_k$ zu berechnen. Die sequentiell linearisierten Polynome $g_1, \ldots, g_k$ in den ursprünglichen Variablen $y_1, \ldots, y_k$ sind ein Teil des geheimen Schlüssels. Sukzessive können daher die Werte für $y_1, \ldots, y_k$ berechnet werden. Mit Hilfe der Beziehung

$$\begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix} = A^{-1} \cdot \begin{pmatrix} y_1 \\ \vdots \\ y_k \end{pmatrix}$$

werden die Werte für die Variablen $x_1, \ldots, x_k$ ermittelt.

Die berechneten Werte für $x_1, \ldots, x_k$ hängen von einem zufälligen Wert für f_1 ab. Es gibt deshalb für jede Nachricht viele gültige Unterschriften. Diese Nicht-Eindeutigkeit der Signaturen verhindert Interpolationsangriffe.

Fortsetzung des Beispiels Die Werte, die sich durch Anwendung der Hashfunktionen auf die Nachricht m ergeben, seien $h_2(m) = 357$, $h_3(m) = 491$. Der zufällige Wert für $f_1(x_1, \ldots, x_k)$ sei 218. Es gilt also

$$\begin{pmatrix} f_1 \\ f_2 \\ f_3 \end{pmatrix} = \begin{pmatrix} 218 \\ 357 \\ 491 \end{pmatrix}.$$

Für die Inversen der Matrizen A, B gilt:

$$A^{-1} = \begin{pmatrix} 813 & 372 & 614 \\ 187 & 171 & 541 \\ 205 & 385 & 309 \end{pmatrix}, \quad B^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 746 & 571 \\ 0 & 556 & 377 \end{pmatrix}.$$

Daraus folgt

$$\begin{pmatrix} g_1 \\ g_2 \\ g_3 \end{pmatrix} = B^{-1} \cdot \begin{pmatrix} f_1 \\ f_2 \\ f_3 \end{pmatrix} = \begin{pmatrix} 218 \\ 91 \\ 625 \end{pmatrix}$$

Mit Hilfe der sequentiell linearisierten Polynome g_1, g_2, g_3 ergibt sich $y_1 = 218$, $y_2 = 153$, $y_3 = 614$. Transformiere diese Zahlen in Werte für x_1, x_2, x_3:

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = A^{-1} \cdot \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = \begin{pmatrix} 725 \\ 846 \\ 247 \end{pmatrix}$$

Die Zuweisung $x_1 = 725$, $x_2 = 846$, $x_3 = 247$ bildet eine gültige Signatur für die Nachricht. Beim Einsetzen in die Polynome des öffentlichen Schlüssels ergeben sich die Werte der Hashfunktionen. □

Kapitel 3

Der Angriff auf das Schema der sequentiellen Linearisierung

Die Darstellung des Angriffs folgt den Ausführungen von Coppersmith, Stern und Vaudenay (1993).

3.1 Mathematische Hilfsmittel

3.1.1 Quadratische Formen

Sei K ein Körper mit von zwei verschiedener Charakteristik. Jeder homogenen quadratischen Form $q(x) = q(x_1, \ldots, x_k) \in K[x_1, \ldots, x_k]$ wird eine symmetrische $k \times k$-Matrix Q mit $q(x) = x^T Q x$ zugeordnet:

$$Q_{j,l} := \begin{cases} \text{Koeffizient von } x_j x_l \text{ in } q, & j = l \\ \frac{1}{2} \cdot \text{Koeffizient von } x_j x_l \text{ in } q, & j \neq l \end{cases} . \tag{3.1}$$

Q heißt die **Formenmatrix** von q (siehe Bronstein (1989)).

Definition 3.1 1. Der **Kern einer quadratischen Form** sei definiert als der Kern der zugehörigen Formenmatrix:

$$\text{Kern } q := \text{Kern } Q = \{x \in K^k : Qx = 0\}$$

2. Der **Rang einer quadratischen Form** sei definiert als der Rang der zugehörigen Formenmatrix.

Man beachte, bei dieser Definition der Kern einer quadratischen Form q nicht identisch mit der Menge

$$\{x \in K^k : q(x) = 0\}$$

ist.

Lemma 3.2 Sei $q(x) = x^T Q x$ eine quadratische Form.

1. Aus $x \in \text{Kern } q$ folgt $q(x) = 0$.

2. Sei $x = A \cdot y$ eine invertierbare lineare Variablentransformation. Die transformierte quadratische Form habe die Formenmatrix D. Dann gilt

$$\det D = (\det A)^2 \cdot \det Q.$$

Die Dimension des Kerns und der Rang der quadratischen Form sind invariant gegenüber der invertierbaren linearen Variablentransformation.

Beweis 1. Sei $x \in \text{Kern } q$. Dann gilt

$$q(x) = x^T Q x = x^T \vec{0} = 0.$$

2. Es gilt

$$q(x) = x^T Q x = (Ay)^T Q (Ay) = y^T (A^T Q A) y$$

und damit

$$\det D = \det(A^T Q A) = (\det A)^2 \det Q.$$

Die Invarianz der Kerndimension und des Rangs folgt aus der Tatsache, daß Q und $A^T Q A$ den gleichen Rang haben. □

3.1.2 Das Pollard-Verfahren

Pollard und Schnorr (1987) haben einen Algorithmus entwickelt, mit dem Kongruenzen der Form

$$x^2 + ky^2 = m \pmod{n}$$

in probabilistischer Polynomialzeit gelöst werden können, ohne daß die Faktorisierung des Moduls n bekannt sein muß. Voraussetzung für die Anwendung des Verfahrens ist, daß m und k teilerfremd zu n sind.

Der Algorithmus läßt sich wie folgt skizzieren (siehe auch Brickell und Odlyzko (1988)):

1. Führe die Schritte 2. und 3. so lange aus, bis die ganze Zahl m eine Quadratzahl in $\mathbb{Z}$ ist oder das Paar $(k, m) = (-1, -1)$ ist. Im Falle der Quadratzahl wird die Gleichung durch Wahl von $y = 0$ direkt gelöst, in dem speziellen Fall kann die Gleichung durch $x = 0$ und $y = 1$ gelöst werden.

2. Ersetze m durch eine äquivalente Zahl m', so daß $m' < 2\sqrt{|k|}$.

3. Substituiere $x = x'/y'$ und $y = 1/y'$. Multipliziert man die dadurch entstehende Gleichung mit y'^2, erhält man die Gleichung $x'^2 - m'y'^2 = -k$. Die Rollen von m' und k' sind also vertauscht worden. Die rechte Seite der Gleichung läßt sich durch eine rekursive Anwendung des Verfahrens erneut verkleinern.

4. Nach dem Lösen eines der in 1. beschriebenen Gleichungstypen verwendet man die Transformationen, um zurück zur Ausgangsgleichung zu schließen.

In Schritt 2 wird der folgende Zusammenhang verwendet: Seien $x_1^2 + ky_1^2 = m_1$ und $x_2^2 + ky_2^2 = m_2$ Polynomgleichungen in x_1, y_1 bzw. x_2, y_2. Sei $x := x_1x_2 - ky_1y_2$ und $y := x_1y_2 + x_2y_1$. Dann gilt

$$x^2 + ky^2 = m_1m_2. \tag{3.2}$$

Skizze von Schritt 2:

2.a Suche eine Primzahl $m_0 \in \mathbb{Z}$, so daß $m_0 = m \pmod n$ und $-k$ ein quadratischer Rest modulo m_0 ist.

2.b Löse $x_0^2 = -k \pmod{m_0}$. Berechne die Zahl $m_1 \in \mathbb{Z}$, für die $x_0^2 + k = m_0m_1$ gilt.

2.c Reduziert man eine Basis des zweidimensionalen Gitters

$$L = \left\{ (u, \sqrt{|k|}v) \;\middle|\; x_0v = u \pmod{m_1} \right\}$$

im Sinne von Gauß bzw. von Lenstra, Lenstra, Lovász (1982), so erhält man einen kürzesten Gittervektor (x_1, y_1). Setzt man $m' := (x_1^2 + ky_1^2)/m_1$, so gilt $m' < 2\sqrt{|k|}$.

2.d Das Ausgangsproblem reduziert sich auf das Lösen von $x_2^2 + ky_2^2 = m' \pmod n$. Die Lösungen der drei Gleichungen

$$\begin{aligned} x_0^2 + k &= m_0m_1, \\ x_1^2 + ky_1^2 &= m_1m', \\ x_2^2 + ky_2^2 &= m' \end{aligned}$$

können mit Hilfe der Gleichung (3.2) zu einer Lösung für $x^2 + ky^2 = m \pmod n$ zusammengesetzt werden.

Durch die Anwendung affiner Variablentransformationen lassen sich mit Hilfe des Pollard-Verfahrens allgemeinere quadratische Kongruenzen effizient lösen:

Satz 3.3 (Adleman, Estes, McCurley (1987)) Sei n eine ungerade positive Zahl,

$$\begin{aligned} f(x,y) &= Ax^2 + Bxy + Cy^2 + Dx + Ey + F \\ \text{und } \Delta(f) &= \det \begin{pmatrix} 2A & B & D \\ B & 2C & E \\ D & E & 2F \end{pmatrix}. \end{aligned}$$

Wenn $\gcd(\Delta(f), n) = 1$ ist, dann existiert für jedes $\epsilon > 0$ ein Algorithmus, der die Kongruenz $f(x, y) = 0 \pmod{n}$ mit einer Wahrscheinlichkeit von mindestens $1 - \epsilon$ löst und dessen Laufzeit nur polynomial von der Bitlänge des Moduls n abhängt.

3.2 Idee des Angriffs

Bei diesem Angriff zielen wir nicht auf die Rekonstruktion der geheimen Transformationen. Stattdessen erzeugen wir direkt vom öffentlichen Schlüssel eine gültige Signatur für die Nachricht.

Es werden Eigenschaften der Polynome genutzt, die unter den durchgeführten Transformationen invariant bleiben. Wir erhalten dadurch Informationen über den geheimen Schlüssel, die es erlauben, Teile der Transformationen rückgängig zu machen. Obwohl der geheime Schlüssel nicht entdeckt wird, können Gleichungen ermittelt werden, die in Verbindung mit dem Pollard-Verfahren zum Generieren einer Unterschrift ausreichen.

Wir betrachten zunächst den Fall, daß der Modul n eine Primzahl ist. Im Anschluß daran wird dargelegt, warum die Überlegungen auch im Falle eines zusammengesetzten Moduls der Form $n = p \cdot q$ anwendbar sind.

Weiterhin werden wir uns darauf beschränken, nur nicht-entartete Fälle zu betrachten. Zum Brechen eines kryptographischen Systems genügt es, einen substantiellen Anteil der Schlüsselpaare des Systems zu brechen. Für den Angriff seien die folgenden Voraussetzungen erfüllt. In Abschnitt 3.5 werden die Voraussetzungen beurteilt.

Nicht-Entartungsbedingungen 3.4

1. Sei $g_1, \ldots, g_k$ das in (2.1) eingeführte System der sequentiell linearisierten Polynome.
   Forderung: Die quadratische Form g_i habe den Rang i, $2 \leq i \leq k$.

2. Im Verlauf des Angriffs wird der Quotient zweier unbekannter Koeffizienten δ_i und δ_k aus $\mathbb{Z}_n$ gebildet.
   Forderung: δ_k sei ungleich Null.

3. Im Verlauf des Angriffs werden Polynome konstruiert, von denen bekannt ist, daß eine doppelte Nullstelle vorliegt. Sei $p(x)$ ein solches Polynom.
   Forderung: $p(x)$ besitze genau eine Nullstelle mit einer Vielfachheit größer als 1.

4. Im Verlauf des Angriffs werden quadratische Formen linear miteinander kombiniert, so daß die resultierende quadratische Form $\tilde{f}_i$ einen Rang kleiner als k hat.
   Forderung: $\tilde{f}_i$ hat den Rang $k - 1$.

5. Im vorletzten Schritt des Angriffs wird mit Hilfe des Pollard-Verfahrens die Lösung einer allgemeinen quadratischen Kongruenz in zwei Unbekannten bestimmt.
   Forderung: Die Voraussetzungen für die Anwendung des Pollard-Verfahrens aus Satz 3.3 seien erfüllt.

6. Im letzten Schritt des Angriffs wird ein sequentiell linearisiertes Gleichungssystem aufgelöst.
   Forderung: Bei der Auflösung des Gleichungssystems trete keine Division durch Null auf.

3.3 Fälschen einer Unterschrift

Sei $g_1, \ldots, g_k$ das in (2.1) eingeführte System der sequentiell linearisierten Polynome.

Bezeichnung 3.5 Sei $2 \leq i \leq k$. Mit K_i bezeichnen wir den Kern der quadratischen Form g_i, $2 \leq i \leq k$.

Ebenso wie die quadratische Form g_i selbst läßt sich der Kern K_i in den ursprünglichen und in den neuen Variablen beschreiben, $2 \leq i \leq k$.

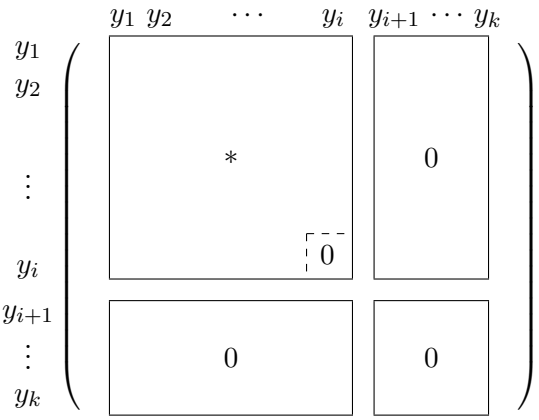
Lemma 3.6 1. In den ursprünglichen Variablen läßt sich K_i wie folgt ausdrücken:

$$K_i = \Big\{(y_1, \ldots, y_k)^T : y_1 = \ldots = y_i = 0\Big\}, \quad 2 \leq i \leq k.$$

2. $\dim K_i = k - i, \quad 2 \leq i \leq k.$

3. Sei $y \in K_{i-1}$. Dann ist $g_i(y) = 0, \quad 3 \leq i \leq k.$

Beweis 1. Für $i \in \{2, \ldots, k\}$ sei G_i die nach (3.1) zugeordnete Formenmatrix von g_i. Wegen der sequentiellen Linearisierung der Polynome $g_1, \ldots, g_k$ hat G_i die folgende Form:



Sei H_i die linke obere $i \times i$-Teilmatrix von G_i. Es gilt

$$\begin{aligned} K_i &= \Big\{(y_1, \ldots, y_k)^T : G_i \cdot (y_1, \ldots, y_k)^T = 0\Big\} \\ &= \Big\{(y_1, \ldots, y_k)^T : \forall l \in \{1, \ldots, k\} \sum_{j=1}^{k} (G_i)_{lj}\, y_j = 0\Big\} \end{aligned}$$

$$
\begin{aligned}
&= \Big\{(y_1,\ldots,y_k)^T : \forall l \in \{1,\ldots,i\} \sum_{j=1}^{i} (G_i)_{lj}\, y_j = 0\Big\} \\
&= \Big\{(y_1,\ldots,y_k)^T : (y_1,\ldots,y_i)^T \in \mathrm{Kern}(H_i)\Big\}
\end{aligned}
$$

Wegen der Nicht-Entartung hat die Matrix G_i den Rang i. Es folgt, daß die Matrix H_i regulär ist und damit

$$K_i = \Big\{(y_1,\ldots,y_k)^T : y_1 = \ldots = y_i = 0\Big\}.$$

2. Diese Aussage folgt unmittelbar aus der im ersten Teil gefundenen Aussage für K_i.

3. Für ein $y \in K_{i-1}$ gilt aufgrund der ersten Aussage $y_1 = \ldots = y_{i-1} = 0$. Die quadratische Form g_i hat nach (2.1) die Form

$$g_i(y_1,\ldots,y_k) = l_i(y_1,\ldots,y_{i-1}) \cdot y_i + q_i(y_1,\ldots,y_{i-1}).$$

Sowohl die homogene lineare Funktion l_i als auch die homogene quadratische Funktion q_i hängen nur von den Variablen $y_1,\ldots,y_{i-1}$ ab und sind damit Null. □

Wir werden nun die unbekannten Koeffizienten δ_i der Linearkombinationen

$$f_i = \delta_i g_k + \sum_{j=2}^{k-1} \beta_{ij} g_j, \quad 2 \le i \le k,$$

genauer untersuchen.

Zu diesem Zweck definieren wir

$$d_i^\lambda := f_i - \lambda f_k, \quad 2 \le i < k.$$

d_i^λ ist eine quadratische Form mit dem linearen Parameter λ. Die Formenmatrix D_i^λ der quadratischen Form d_i^λ hat in den ursprünglichen Variablen die Form

$$
D_i^\lambda = \begin{array}{c}
\begin{array}{cccccc} y_1 & y_2 & & \cdots & y_{k-1} & y_k \end{array} \\
\left(\begin{array}{|ccc|c|} \hline & & & & \\ & * & & & U_i^\lambda \\ & & & & \\ \hline (U_i^\lambda)^T & & & & 0 \\ \hline \end{array}\right)
\end{array}
$$

mit einer $(k-1) \times 1$-Matrix U_i^λ. Jeder Eintrag von U_i^λ ist eine affine Funktion in λ.

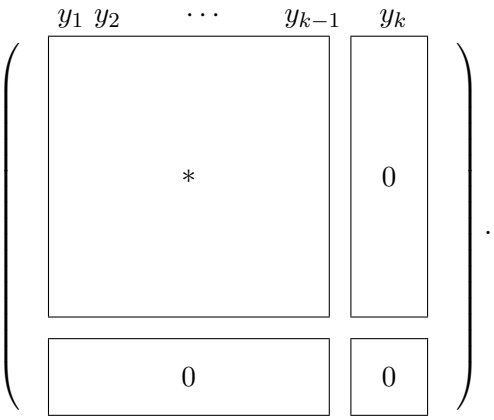
Wir setzen nun voraus, daß δ_k ungleich Null ist. Im nicht-entarteten Fall ist diese Voraussetzung gerechtfertigt (siehe Forderung 2). Für

$$\lambda_i := \frac{\delta_i}{\delta_k} \tag{3.3}$$

gilt

$$d_i^{\lambda_i} = \sum_{j=2}^{k-1} \beta_{ij} g_j - \frac{\delta_i}{\delta_k} \sum_{j=2}^{k-1} \beta_{kj} g_j.$$

$d_i^{\lambda_i}$ ist also unabhängig von g_k. Aufgrund der sequentiellen Linearisierung hängen die Polynome $g_1, \ldots, g_{k-1}$ nicht von der Variablen y_k ab. Folglich ist $d_i^{\lambda_i}$ unabhängig von y_k. Die Formenmatrix D_i^λ an der Stelle $\lambda = \lambda_i$ hat deshalb die Form



Jeder Eintrag von U_i^λ ist eine affin-lineare Funktion in λ, welche an der Stelle $\lambda = \lambda_i$ verschwindet. Wir können jeden Eintrag von U_i^λ daher in der Form

$$\text{Faktor} \cdot (\lambda - \lambda_i)$$

schreiben.

Sei nun

$$P_i(\lambda) := \det(D_i^\lambda). \tag{3.4}$$

Durch Entwicklung dieser Determinante nach der letzten Spalte und der letzten Zeile spaltet sich der Faktor $(\lambda - \lambda_i)^2$ ab. Die doppelte Nullstelle λ_i tritt nach Lemma 3.2 auch bezüglich der neuen Variablen $x_1, \ldots, x_k$ auf.

Zur Berechnung der doppelten Nullstelle λ_i wird der größte gemeinsame Teiler von $P_i(\lambda)$ und $P_i'(\lambda)$ ermittelt. Im nicht-entarteten Fall gilt (siehe Forderung 3): Die Vielfachheit der beschriebenen Nullstelle ist nicht größer als 2, und alle anderen Nullstellen von $P_i(\lambda)$ haben die Vielfachheit 1. Dies liefert ein lineares Polynom in λ mit der Nullstelle λ_i.

Nach der Berechnung von $\lambda_2, \ldots, \lambda_{k-1}$ setzen wir

$$\begin{aligned} \tilde{f}_i &= f_i - \lambda_i f_k, \quad 2 \le i \le k-1, \\ \text{und } \tilde{f}_k &= f_k. \end{aligned}$$

Lemma 3.7 Für die quadratischen Formen $\tilde{f}_i$, $2 \leq i \leq k-1$, gilt

1. Kern $\tilde{f}_i = K_{k-1}$,
2. $\tilde{f}_i$ ist eine Linearkombination der Polynome $g_2, \ldots, g_{k-1}$.

Beweis 1. Die letzte Zeile und die letzte Spalte der Formenmatrix von $\tilde{f}_i$ in den ursprünglichen Variablen $y_1, \ldots, y_k$ enthält nur Nullen. Im nicht-entarteten Fall gemäß Forderung 4 ist $\tilde{f}_i$ eine quadratische Form vom Rang $k-1$. Es gilt

$$\text{Kern } \tilde{f}_i = \{(y_1, \ldots, y_k) : y_1 = \ldots = y_{k-1} = 0\} = K_{k-1}, \quad 2 \leq i \leq k-1.$$

2. Die letzte Zeile und die letzte Spalte der Formenmatrix von $\tilde{f}_i$ in den ursprünglichen Variablen $y_1, \ldots, y_k$ enthält nur Nullen. $\tilde{f}_i$ ist daher unabhängig von y_k. g_k hängt von y_k echt ab, weil die lineare Funktion l_k aus (2.1) nicht die Nullfunktion ist. Deshalb ist $\tilde{f}_i$ eine Linearkombination der Polynome $g_2, \ldots, g_{k-1}$. □

Sei c_k ein Vektor, der den eindimensionalen Kern K_{k-1} bzgl. der neuen Variablen aufspannt. Die $k-1$ Polynome $\tilde{f}_2, \ldots, \tilde{f}_{k-1}$, die Linearkombinationen der $k-1$ sequentiell linearisierten Polynome $g_2, \ldots, g_{k-1}$ sind, bilden ein Problem kleinerer Ordnung.

Damit das Problem formal um eine Stufe reduziert wird, muß auch die Dimension des zugrundeliegenden Raumes verkleinert werden. In den ursprünglichen Variablen könnten einfach die letzte Zeile und die letzte Spalte der Formenmatrix entfernt werden, da sie wegen der Unabhängigkeit von y_k nur aus Nullen bestehen.

Wir konstruieren eine Matrix C, die die neuen Variablen $x_1, \ldots, x_k$ so transformiert, daß $\tilde{f}_2, \ldots, \tilde{f}_{k-1}$ nur noch von $k-1$ Variablen abhängen. Zu diesem Zweck führen wir die Variablen $z_1, \ldots, z_k$ ein.

Konstruiere C wie folgt:

- Die letzte Spalte von C enthalte den Vektor c_k.
- Die ersten $k-1$ Spalten von C sind so zu wählen, daß die Matrix C regulär ist.

Die lineare Variablentransformation

$$x = C \cdot z$$

bildet den k-ten Einheitsvektor bzgl. der z-Koordinaten auf den Vektor c_k bzgl. der x-Koordinaten ab. Die jeweils letzte Zeile und letzte Spalte der Formenmatrizen von $\tilde{f}_2, \ldots, \tilde{f}_{k-1}$ in den z-Koordinaten bestehen deshalb nur aus Nullen. In den z-Koordinaten kann daher die letzte Zeile und die letzte Spalte der Formenmatrizen entfernt werden. Formal bedeutet das, daß der $(k-1)$-dimensionale Quotientenraum von $\mathbb{Z}_n^k$ nach dem Kern K_{k-1} betrachtet wird.

Wir setzen die beschriebene Konstruktion induktiv fort. In jedem Schritt werden die quadratischen Formen $\tilde{f}_2, \ldots \tilde{f}_{k-1}$ anstelle von $f_2, \ldots, f_k$ verwendet. Am Ende erhalten wir eine Folge von Vektoren c_i, $3 \leq i \leq k$, für die gilt:

$$c_{i+1}, \ldots, c_k \text{ spannt } K_i \text{ auf }, \quad 2 \leq i \leq k-1.$$

Lemma 3.8 Für die quadratischen Formen $\tilde{f}_2, \ldots, \tilde{f}_k$ und die Vektoren $c_3, \ldots, c_k$ gilt

1. $\tilde{f}_i$ hat den Kern K_i, $\quad 2 \leq i \leq k-1$.
2. $\tilde{f}_i(c_i) = 0, \quad 3 \leq i \leq k$.

Beweis 1. Diese Aussage folgt aus Lemma 3.7 und der induktiven Konstruktion.

2. Aufgrund der induktiven Konstruktion ist $\tilde{f}_i$ eine Linearkombination der Polynome $g_2, \ldots, g_i$. Da c_i im Kern von $g_2, \ldots, g_{i-1}$ liegt, gilt $g_2(c_i) = 0, \ldots, g_{i-1}(c_i) = 0$. Aufgrund der dritten Aussage von Lemma 3.6

$$y \in K_{i-1} \Longrightarrow g_i(y) = 0$$

gilt auch $g_i(c_i) = 0$. Es folgt $\tilde{f}_i(c_i) = 0$. □

Wähle Vektoren c_1 und c_2, so daß die Matrix $C = (c_1, \ldots, c_k)$ regulär ist. Betrachte die Transformationsmatrix

$$C = (c_1, \ldots, c_k).$$

Für die Variablentransformation

$$x = C \cdot z = (c_1, \ldots, c_k) \cdot z$$

gilt, daß der j-te Einheitsvektor bzgl. der z-Koordinaten auf den Vektor c_j bzgl. der x-Koordinaten abgebildet wird, $3 \leq j \leq k$.

Lemma 3.9 Es gilt

1. $\tilde{f}_2$ ist eine quadratische Form in z_1, z_2.
2. $\tilde{f}_3, \ldots, \tilde{f}_k$ sind sequentiell linearisiert.

Beweis $\tilde{f}_2$ hat den Kern K_2, daher werden die Komponenten $z_3, \ldots, z_k$ in den Kern von $\tilde{f}_2$ abgebildet. Die Aussage, daß z_i nur linear in $\tilde{f}_i$ auftritt, folgt aus der Tatsache, daß $\tilde{f}_i(c_i) = 0$ ist. □

Im nicht-entarteten Fall kann die quadratische Kongruenz für $\tilde{f}_2$ mit der Pollard-Methode gelöst werden (siehe Forderung 5).

Die Werte für $z_3, \ldots, z_k$ können im nicht-entarteten Fall sukzessive mit Hilfe der sequentiell Polynome $\tilde{f}_3, \ldots, \tilde{f}_k$ gefunden werden (siehe Forderung 6). Mittels $x = C \cdot z$ kann aus der Belegung des Vektors z die Belegung des Vektors x ermittelt werden.

Damit haben wir ohne Kenntnis des geheimen Schlüssels eine gültige Unterschrift erzeugt.

3.4 Zusammengesetzte Moduln

Das Verfahren gilt in der beschriebenen Weise nur für prime Moduln. Sei n nun ein Modul der Form $p \cdot q$. Mit Hilfe des Chinesischen Restsatzes lassen sich alle Überlegungen auf den zusammengesetzten Modul übertragen. Beim Auftreten nicht-invertierbarer Elemente im Ring der ganzen Zahlen modulo n kommt es zu einer Ausnahme. Das Auftreten nicht-invertierbarer Element außer der Null liefert jedoch die Faktorisierung des Moduls.

3.5 Sonderfälle

In diesem Abschnitt sollen die Voraussetzungen für den nicht-entarteten Fall aus Definition 3.4 beurteilt werden. Die Zahl k der Variablen sei klein, zum Beispiel $k \in \{3, \ldots, 10\}$.

Zu Forderung 1 (sie wird im Beweis von Lemma 3.6 benutzt). Bei zufälliger Wahl des geheimen Schlüssels ist die Forderung mit großer Wahrscheinlichkeit erfüllt.

Zu Forderung 2 (sie wird in Gleichung (3.3) benutzt). Der Hauptteil des Angriffs wird $(k-2)$-mal durchlaufen. Bei zufälliger Wahl des geheimen Schlüssels ist die Forderung in jedem dieser Durchläufe mit großer Wahrscheinlichkeit erfüllt.

Zu Forderung 3 (sie wird bei der Analyse des Polynoms aus (3.4) benutzt). Für ein zufällig gewähltes Polynom $p(x)$ ist die Forderung mit großer Wahrscheinlichkeit erfüllt. Wir vermuten, daß die Forderung auch für die Polynome, die in dem Verfahren auftreten, mit großer Wahrscheinlichkeit erfüllt ist.

Zu Forderung 4 (sie wird im Beweis von Lemma 3.7 benutzt). Die Polynome f_i sind Linearkombinationen der sequentiell linearisierten Polynome g_i. Bei zufälliger Wahl des geheimen Schlüssels ist die Forderung mit großer Wahrscheinlichkeit erfüllt.

Zu Forderung 5 (sie wird im vorletzten Schritt des Verfahrens benutzt). Für zufällig gewählte quadratische Kongruenzen gewährleistet Satz 3.3, daß die Forderung mit großer Wahrscheinlichkeit erfüllt ist. Wir vermuten, daß die Forderung auch für die Kongruenzen, die in dem Verfahren auftreten, mit großer Wahrscheinlichkeit erfüllt ist.

Zu Forderung 6 (sie wird im letzten Schritt des Verfahrens benutzt). Wir vermuten, daß das konstruierte sequentiell linearisierte Gleichungssystem mit großer Wahrscheinlichkeit die Forderung erfüllt.

Leider können wir die entarteten Schlüsselpaare **nicht** unabhängig von dem beschriebenen Angriff charakterisieren. Wir vermuten, daß der Anteil der entarteten Schlüsselpaare sehr gering ist.

3.6 Beispiele

Beispiel 3.10 Es werden die gleichen Schlüssel wie in Beispiel 2.4 verwendet.

Die quadratischen Formen f_2, f_3 lassen sich wie folgt notieren:

$$f_2 = x^T \begin{pmatrix} 777 & 111 & 604 \\ 111 & 332 & 718 \\ 604 & 718 & 181 \end{pmatrix} x, \quad f_3 = x^T \begin{pmatrix} 553 & 96 & 140 \\ 96 & 435 & 150 \\ 140 & 150 & 559 \end{pmatrix} x.$$

Für eine quadratische Form q bezeichnet $\mathrm{Mat}(q)$ die zugehörige Formenmatrix. Es folgt

$$\begin{aligned} P_2(\lambda) &= \det(\mathrm{Mat}(f_2 - \lambda f_3)) = 464 + 853\lambda + 698\lambda^2 + 191\lambda^3, \\ P_2'(\lambda) &= 853 + 497\lambda + 573\lambda^2, \\ \gcd(P_2, P_2') &= \lambda - 133, \\ \lambda_2 &= 133. \end{aligned}$$

Definiere

$$\tilde{f_2} := f_2 - 133 f_3, \quad \tilde{f_3} := f_3.$$

Der Kern von

$$\mathrm{Mat}(\tilde{f_2}) = \begin{pmatrix} 47 & 828 & 863 \\ 828 & 13 & 546 \\ 863 & 546 & 451 \end{pmatrix}$$

wird durch $c_3 = (130, 668, 1)^T$ aufgespannt. Wähle zufällig $c_2 = (0, 1, 0)^T$, $c_1 = (1, 2, 0)^T$.

$$C := (c_1, c_2, c_3) = \begin{pmatrix} 1 & 0 & 130 \\ 2 & 1 & 668 \\ 0 & 0 & 1 \end{pmatrix}, \quad x = C \cdot z.$$

$\tilde{f_2}$, $\tilde{f_3}$ lauten in den x- und den z-Variablen

$$\begin{aligned} \tilde{f_2} &= 47x_1^2 + 757x_1x_2 + 13x_2^2 + 827x_1x_3 + 193x_2x_3 + 451x_3^2 \\ &= 714z_1^2 + 809z_1z_2 + 13z_2^2, \\ \tilde{f_3} &= 553x_1^2 + 192x_1x_2 + 435x_2^2 + 280x_1x_3 + 300x_2x_3 + 559x_3^2 \\ &= 879z_1^2 + 134z_1z_2 + 435z_2^2 + (8z_1 + 494z_2)z_3. \end{aligned}$$

Löse die Gleichung

$$\tilde{f_2} = 714z_1^2 + 809z_1z_2 + 13z_2^2 = h_2(m) - 133h_3(m) = 681$$

mit der Pollard-Methode, und berechne dann z_3 aus der Gleichung

$$\tilde{f_3} = 879z_1^2 + 134z_1z_2 + 435z_2^2 + (8z_1 + 494z_2)z_3 = h_3(m) = 491.$$

Sei zum Beispiel

$$z_1 = 465, \quad z_2 = 443$$

eine durch das Pollard-Verfahren generierte Lösung. Dann ist $z_3 = 177$. Der Vektor

$$x = C \cdot z = \begin{pmatrix} 101 \\ 42 \\ 177 \end{pmatrix}$$

bildet eine gültige Unterschrift für die Nachricht m.

Beispiel 3.11 In dem nachfolgenden Angriff mit $k = 4$ kommt die induktive Arbeitsweise des Verfahrens zum Ausdruck. Wie im vorangegangenen Beispiel sei der Modul $n = 31 \cdot 29 = 899$.

Die sequentiell linearisierten Ausgangsgleichungen

$$\begin{aligned} g_1 &= y_1, \\ g_2 &= y_1 y_2, \\ g_3 &= 782y_1^2 + 675y_1y_2 + 249y_2^2 + (112y_1 + 385y_2)y_3, \\ g_4 &= 393y_1^2 + (820y_1 + 145y_2)y_2 + (794y_1 + 284y_2 + 647y_3)y_3 \\ &\quad +(752y_1 + 247y_2 + 852y_3)y_4 \end{aligned}$$

und die beiden linearen Transformationen

$$A = \begin{pmatrix} 1 & 456 & 23 & 112 \\ 1 & 593 & 205 & 657 \\ 1 & 873 & 125 & 453 \\ 1 & 37 & 359 & 612 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 435 & 760 & 301 \\ 0 & 422 & 391 & 627 \\ 0 & 765 & 341 & 197 \end{pmatrix}$$

generieren den folgenden öffentlichen Schlüssel:

$$f_2 = x^T \begin{pmatrix} 763 & 512 & 772 & 296 \\ 512 & 856 & 692 & 810 \\ 772 & 692 & 576 & 864 \\ 296 & 810 & 864 & 197 \end{pmatrix} x, \quad f_3 = x^T \begin{pmatrix} 712 & 101 & 30 & 307 \\ 101 & 520 & 60 & 805 \\ 30 & 60 & 889 & 511 \\ 307 & 805 & 511 & 83 \end{pmatrix} x,$$

$$f_4 = x^T \begin{pmatrix} 603 & 892 & 122 & 524 \\ 892 & 219 & 599 & 742 \\ 122 & 599 & 586 & 837 \\ 524 & 742 & 837 & 281 \end{pmatrix} x.$$

Die Hashwerte für die Nachricht m seien

$$h_2(m) = 357, \quad h_3(m) = 491, \quad h_4(m) = 297.$$

Es folgt

$$\begin{aligned} P_2(\lambda) &= 416 + 767\lambda + 424\lambda^2 + 893\lambda^3 + 709\lambda^4, \\ P_2'(\lambda) &= 767 + 848\lambda + 881\lambda^2 + 139\lambda^3, \\ \gcd(P_2, P_2') &= \lambda - 467, \\ \lambda_2 &= 467. \end{aligned}$$

$$\begin{aligned} P_3(\lambda) &= 409 + 118\lambda + 533\lambda^2 + 600\lambda^3 + 709\lambda^4, \\ P_3'(\lambda) &= 118 + 167\lambda + 2\lambda^2 + 139\lambda^3, \\ \gcd(P_3, P_3') &= \lambda - 26, \\ \lambda_3 &= 26. \end{aligned}$$

Definiere

$$\begin{aligned} \tilde{f}_2 &= f_2 - 467 f_4, \\ \tilde{f}_3 &= f_3 - 26 f_4, \\ \tilde{f}_4 &= f_4. \end{aligned}$$

Die Formenmatrizen

$$\mathrm{Mat}(\tilde{f}_2) = \begin{pmatrix} 549 & 185 & 435 & 116 \\ 185 & 170 & 548 & 411 \\ 435 & 548 & 210 & 151 \\ 116 & 411 & 151 & 224 \end{pmatrix} \text{ und } \mathrm{Mat}(\tilde{f}_3) = \begin{pmatrix} 317 & 283 & 454 & 168 \\ 283 & 220 & 668 & 392 \\ 454 & 668 & 37 & 325 \\ 168 & 392 & 325 & 868 \end{pmatrix}$$

haben den gleichen Kern. Er wird durch den Vektor $c_4 = (415, 115, 355, 1)^T$ aufgespannt. Wähle für die c_1, c_2, c_3 die ersten drei Einheitsvektoren.

$$C := (c_1, c_2, c_3, c_4) = \begin{pmatrix} 1 & 0 & 0 & 415 \\ 0 & 1 & 0 & 115 \\ 0 & 0 & 1 & 355 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad x = C \cdot z.$$

Damit ist

$$\tilde{f}_2 = z^T \begin{pmatrix} 549 & 185 & 435 & 0 \\ 185 & 170 & 548 & 0 \\ 435 & 548 & 210 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} z, \quad \tilde{f}_3 = z^T \begin{pmatrix} 317 & 283 & 454 & 0 \\ 283 & 220 & 668 & 0 \\ 454 & 668 & 37 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} z.$$

Die während der zweiten Anwendung des Verfahrens gefundenen Werte werden durch einen Unterstrich gekennzeichnet. Bei der Ermittlung der doppelten Nullstelle $\underline{\lambda_2}$ ergibt sich

$$\begin{aligned} \underline{P_2}(\lambda) &= 648 + 473\lambda + 19\lambda^2 + 163\lambda^3, \\ \underline{P_2'}(\lambda) &= 473 + 38\lambda + 489\lambda^2, \\ \gcd(\underline{P_2}, \underline{P_2'}) &= \lambda - 195, \\ \underline{\lambda_2} &= 195. \end{aligned}$$

Definiere

$$\begin{aligned} \underline{\tilde{f}_2} &= \tilde{f}_2 - 195 f_3, \\ \underline{\tilde{f}_3} &= \tilde{f}_3, \\ \underline{\tilde{f}_4} &= \tilde{f}_4. \end{aligned}$$

Die Formenmatrix

$$\mathrm{Mat}(\underline{\tilde{f}_2}) = \begin{pmatrix} 765 & 738 & 7 & 619 \\ 738 & 422 & 643 & 386 \\ 7 & 643 & 187 & 605 \\ 619 & 386 & 605 & 875 \end{pmatrix}$$

hat einen zweidimensionalen Kern. Der bereits bekannte Vektor c_4 sowie der Vektor $\underline{c_3} = (114, 311, 0, 1)^T$ bilden ein Erzeugendensystem für den Kern. Wir führen nun die x-Variablen durch die Transformation

$$\underline{C} = (c_1, c_2, \underline{c_3}, c_4) \cdot \underline{z} = \begin{pmatrix} 1 & 0 & 114 & 415 \\ 0 & 1 & 311 & 115 \\ 0 & 0 & 0 & 355 \\ 0 & 0 & 1 & 1 \end{pmatrix} \cdot \underline{z}$$

in neue Variablen $\underline{z_1}, \ldots, \underline{z_k}$ über. In diesen Variablen lauten $\underline{\tilde{f}_2}, \underline{\tilde{f}_3}, \underline{\tilde{f}_4}$

$$\begin{aligned} \underline{\tilde{f}_2} &= 765\underline{z_1}^2 + 577\underline{z_1}\ \underline{z_2} + 422\underline{z_2}^2, \\ \underline{\tilde{f}_3} &= 317\underline{z_1}^2 + 566\underline{z_1}\ \underline{z_2} + 220\underline{z_2}^2 + (514\underline{z_1} + 772\underline{z_2})\underline{z_3}, \\ \underline{\tilde{f}_4} &= 603\underline{z_1}^2 + 885\underline{z_1}\ \underline{z_2} + 219\underline{z_2}^2 + 227\underline{z_1}\ \underline{z_3} + 357\underline{z_2}\ \underline{z_3} + 81\underline{z_3}^2 \\ &\quad +(400\underline{z_1} + 258\underline{z_2} + 225\underline{z_3})\underline{z_4}. \end{aligned}$$

Die rechten Seite für die Gleichungen lassen sich mit Hilfe der durchgeführten Additionen ermitteln.

$$\begin{aligned} \underline{\tilde{f}_2} &= h_2(m) - \lambda_2 h_4(m) - \underline{\lambda_2}(h_3(m) - \lambda_3 h_4(m)) = 517, \\ \underline{\tilde{f}_3} &= h_3(m) - \lambda_3 h_4(m) = 860, \\ \underline{\tilde{f}_4} &= h_4(m) = 297. \end{aligned}$$

Das Pollard-Verfahren berechnet eine Lösung für die quadratische Kongruenz $\underline{\tilde{f}_2} = 517$, zum Beispiel

$$\underline{z_1} = 435, \quad \underline{z_2} = 62.$$

Dann ist $\underline{z_3} = 738$ und $\underline{z_4} = 527$. Der Vektor

$$x = \underline{C} \cdot \underline{z} = (309, 707, 93, 366)^T$$

bildet eine gültige Unterschrift für die Nachricht m.

Kapitel 4

Unterschriften auf der Grundlage algebraischer Basen

Das Schema, das ebenfalls von SHAMIR (1993b) vorgeschlagen wurde, ist sehr allgemein gehalten. SHAMIR hat jedoch einige Varianten hervorgehoben. Wir wollen vorrangig diese Varianten beschreiben und später deren Sicherheit analysieren.

4.1 Mathematische Hilfsmittel

Sei K ein Körper. Dann ist der Begriff der algebraischen Unabhängigkeit gemäß COX, LITTLE, O'SHEA (1992), Paragraph 9.5, wie folgt erklärt:

Definition 4.1 Die Funktionen $g_1, \ldots, g_r \in K[y_1, \ldots, y_k]$ heißen **algebraisch abhängig** über K, wenn es ein Polynom $p \in K[x_1, \ldots, x_r] \setminus \{0\}$ gibt, so daß $p(g_1, \ldots, g_r) = 0$ für alle $(y_1, \ldots, y_k) \in K^k$. Gilt dies nicht, so heißen $g_1, \ldots, g_r$ **algebraisch unabhängig**.

Für unsere Zwecke ist eine geringfügige Modifikation des Begriffs sinnvoll.

Definition 4.2 Die Funktionen $g_1, \ldots, g_r \in K[y_1, \ldots, y_k]$ heißen **strukturell algebraisch abhängig** über K, wenn es ein Polynom $p \in K[x_1, \ldots, x_r] \setminus \{0\}$ gibt, so daß $p(g_1, \ldots, g_r)$ das Nullpolynom in $K[y_1, \ldots, y_k]$ ist. Gilt dies nicht, so heißen $g_1, \ldots, g_r$ **strukturell algebraisch unabhängig**.

Im Falle unendlicher Körper sind die beiden eingeführten Arten der Unabhängigkeit äquivalent. Die Definitionen lassen sich auf beliebige kommutative Ringe R mit Einselement erweitern.

Sei $F_d[y_1, \ldots, y_k]$ die Menge der homogenen Polynome vom Grad d in k Variablen über einem Ring kommutativen Ring R mit Einselement. Im folgenden wird insbesondere $F_2[y_1, \ldots, y_k]$ betrachtet.

Definition 4.3 Eine Menge $G \subseteq F_d[y_1, \ldots, y_k]$ heißt **algebraische Basis** für $F_d[y_1, \ldots, y_k]$, wenn gilt:

1. Die Elemente von G sind strukturell algebraisch unabhängig.
2. Jedes Polynom aus $F_d[y_1, \ldots, y_k]$ läßt sich durch die Elemente aus G, R und die vier Operationen Addition, Subtraktion, Multiplikation und restfreie Division darstellen.

Wir bezeichnen eine Menge G, die die zweite Bedingung erfüllt, als **algebraisches Erzeugendensystem** für $F_d[y_1, \ldots, y_k]$.

Die $k(k+1)/2$ verschiedenen Terme vom Grad 2 sind nicht strukturell algebraisch unabhängig. Diese Tatsache soll ausgenutzt werden, um eine nichtlineare Komponente in ein Unterschriftenschema auf der Grundlage von Polynomgleichungen zu integrieren.

Beispiel 4.4 Sei $k = 3$. Durch y_1y_2, y_1y_3, y_2y_3 lassen sich die Terme y_1^2, y_2^2, y_3^2 und damit alle anderen Polynome aus $F_2[y_1, y_2, y_3]$ ausdrücken:

$$\begin{aligned} y_1^2 &= \frac{(y_1y_2)(y_1y_3)}{(y_2y_3)} \\ y_2^2 &= \frac{(y_1y_2)(y_2y_3)}{(y_1y_3)} \\ y_3^2 &= \frac{(y_1y_3)(y_2y_3)}{(y_1y_2)} \end{aligned}$$

Satz 4.5 Die folgenden Mengen sind algebraische Basen für $F_2[y_1, \ldots, y_k]$:

1. die **symmetrische Basis:** $\{y_1y_2, y_2y_3, y_3y_4, \ldots, y_ky_1\}$, $k \geq 3$ und k ungerade.
2. die **asymmetrische Basis:** $\{y_1^2, y_1y_2, y_2y_3, \ldots, y_{k-1}y_k\}$, $k \geq 1$.
3. die **zentrierte Basis:** $\{y_1^2, y_1y_2, y_1y_3, \ldots, y_1y_k\}$, $k \geq 1$.

Beweis Wir zeigen lediglich, daß die Basen jeden Term y_iy_j mit $i \leq j$ und damit jedes Polynom aus $F_2[y_1, \ldots, y_k]$ generieren können.

1. **Symmetrische Basis:**

Fall 1: $j-i$ ungerade. Die Menge $\{i, i+1, \ldots, j\}$ enthält eine gerade Anzahl von Elementen. Deshalb ist

$$y_iy_j = \frac{(y_iy_{i+1})(y_{i+2}y_{i+3}) \cdot \ldots \cdot (y_{j-1}y_j)}{(y_{i+1}y_{i+2}) \cdot \ldots \cdot (y_{j-2}y_{j-1})}$$

Fall 2: $j - i$ gerade. Da k ungerade ist, enthält die Menge $\{j, j+1, \ldots, k-1, k, 1, \ldots, i\}$ eine gerade Anzahl von Elementen. y_iy_j läßt sich mit Hilfe des Durchlaufs

$$y_iy_j = \frac{(y_jy_{j+1})(y_{j+2}y_{j+3}) \cdot \ldots \cdot (y_{i-1}y_i)}{(y_{j+1}y_{j+2}) \cdot \ldots \cdot (y_{i-2}y_{i-1})}$$

erzeugen.

2. **Asymmetrische Basis:**

Fall 1: $j - i$ ungerade. Wie bei der symmetrischen Basis.

Fall 2: $j - i = 0$. y_1^2 ist in der Basis enthalten. Sukzessive lassen sich durch

$$y_{t+1}^2 = (y_t y_{t+1})^2 / y_t^2$$

die rein quadratischen Elemente erzeugen.

Fall 2: $j - i > 0, j - i$ gerade.

$$y_i y_j = \frac{(y_i y_{i+1})(y_{i+2} y_{i+3}) \cdot \ldots \cdot (y_{j-2} y_{j-1})}{(y_{i+1} y_{i+2}) \cdot \ldots \cdot (y_{j-1} y_j)} \cdot y_j^2$$

3. **Zentrierte Basis:**

$$y_i y_j = \frac{(y_1 y_i)(y_1 y_j)}{y_1^2}$$

□

Folgende zwei Transformationen auf den Elementen einer algebraischen Basis erhalten die Basiseigenschaft:

- lineare Variablentransformationen $Y = AX$ mit einer invertierbaren $k \times k$-Matrix A, wobei $Y = (y_1, \ldots, y_k)^T$ und $X = (x_1, \ldots, x_k)^T$.
- Linearkombinationen der Form $B \cdot G$, wobei B eine invertierbare $k \times k$-Matrix und $G = (g_1, \ldots, g_k)^T$ der Vektor der Basiselemente ist.

4.2 Generieren eines Schlüsselpaares

Zwei lineare, invertierbare Transformationen können eine algebraische Basis einfacher Struktur in eine algebraische Basis komplizierter Struktur überführen. Die beiden Transformationen bilden den privaten Schlüssel, die transformierte algebraische Basis wird als öffentlicher Schlüssel bekanntgegeben.

Seien p, q große Primzahlen, $n := p \cdot q$. Die Teilnehmer des Systems kennen die Faktorisierung des Moduls n nicht. Im folgenden werden alle Rechnungen im Ring der ganzen Zahlen modulo n durchgeführt. Sei $\{g_1, \ldots, g_k\}$ eine algebraische Basis für $F_2[u_1, \ldots, u_k]$.

Variablentransformation: Eine invertierbare Matrix A führt die Variablen $u_1, \ldots, u_k$ in die Variablen $y_1, \ldots, y_k$ über.

$$\begin{pmatrix} u_1 \\ \vdots \\ u_k \end{pmatrix} = A \cdot \begin{pmatrix} y_1 \\ \vdots \\ y_k \end{pmatrix} \tag{4.1}$$

Die Variablen $u_1, \ldots, u_k$ werden im folgenden als die **ursprünglichen Variablen** bezeichnet, die Variablen $y_1, \ldots, y_k$ als die **neuen Variablen**.

Linearkombinationen der Basiselemente: Durch Wahl einer invertierbaren Matrix B werden die Basiselemente $g_1, \ldots, g_k$ in die Basiselemente $v_1, \ldots, v_k$ übergeführt.

$$\begin{pmatrix} v_1 \\ \vdots \\ v_k \end{pmatrix} = B \cdot \begin{pmatrix} g_1 \\ \vdots \\ g_k \end{pmatrix} \tag{4.2}$$

Bei der symmetrischen Basis bedeutet die zweite Transformation

$$\begin{pmatrix} v_1 \\ \vdots \\ v_k \end{pmatrix} = B \cdot \begin{pmatrix} u_1u_2 \\ \vdots \\ u_ku_1 \end{pmatrix}.$$

Durch das Anwenden der beiden Transformationen erhält man k quadratische Formen in den Variablen $y_1, \ldots y_k$. Bei der symmetrischen Basis ergibt sich

$$\begin{aligned} v_i &= \sum_j b_{ij} u_j u_{j+1} \\ &= \sum_j b_{ij} (\sum_l a_{jl} y_l)(\sum_m a_{j+1,m} y_m), \end{aligned} \tag{4.3}$$

wobei die Indizes modulo k zu verstehen sind.

Setzt man nun

$$(C_i)_{jl} = \begin{cases} \text{Koeffizient von } y_j y_l \text{ in (4.3)}, & j = l \\ \frac{1}{2} \cdot \text{Koeffizient von } y_j y_l \text{ in (4.3)}, & j \neq l \end{cases},$$

so erhält man k quadratische Formen

$$v_i = \sum_{j,l} (C_i)_{j,l}\, y_j y_l, \quad C_i \text{ symmetrisch}, \quad 1 \leq i \leq k. \tag{4.4}$$

Die Matrizen $C_1, \ldots, C_{k-1}$ werden bekanntgegeben. Durch das Geheimhalten von C_k gibt es zu jeder Nachricht mehrere gültige Unterschriften.

Beispiel 4.6 Sei $k = 3$, $n = 31 \cdot 29 = 899$. Betrachte die algebraische Basis $\{u_1u_2, u_2u_3, u_3u_1\}$ von $F_2[u_1, u_2, u_3]$ und die linearen Transformationen

$$A = \begin{pmatrix} 567 & 892 & 78 \\ 342 & 847 & 154 \\ 732 & 366 & 274 \end{pmatrix}, \qquad B = \begin{pmatrix} 102 & 471 & 547 \\ 140 & 73 & 825 \\ 698 & 271 & 382 \end{pmatrix}.$$

Die drei Basiselemente lassen sich mittels der Transformationsmatrix A in den neuen Variablen y_1, y_2, y_3 ausdrücken. Alle Rechnungen werden modulo 899 ausgeführt.

$$\begin{aligned}
g_1 = u_1u_2 &= (567y_1 + 892y_2 + 78y_3)(342y_1 + 847y_2 + 154y_3) \\
&= 629y_1^2 + 486y_1y_2 + 364y_2^2 + 720y_1y_3 + 260y_2y_3 + 325y_3^2 \\
g_2 = u_2u_3 &= (342y_1 + 847y_2 + 154y_3)(732y_1 + 366y_2 + 274y_3) \\
&= 422y_1^2 + 804y_1y_2 + 746y_2^2 + 565y_1y_3 + 762y_2y_3 + 842y_3^2 \\
g_3 = u_3u_1 &= (732y_1 + 366y_2 + 274y_3)(567y_1 + 892y_2 + 78y_3) \\
&= 605y_1^2 + 123y_1y_2 + 135y_2^2 + 290y_1y_3 + 559y_2y_3 + 695y_3^2
\end{aligned}$$

Die durch die Matrix B beschriebene Transformation erzeugt die Gleichungen

$$\begin{aligned}
v_1 &= 102g_1 + 471g_2 + 547g_3 \\
&= 515y_1^2 + 188y_1y_2 + 253y_2^2 + 139y_1y_3 + 763y_2y_3 + 797y_3^2 \\
v_2 &= 140g_1 + 73g_2 + 825g_3 \\
&= 378y_1^2 + 760y_1y_2 + 134y_2^2 + 119y_1y_3 + 316y_2y_3 + 697y_3^2 \\
v_3 &= 698g_1 + 271g_2 + 382g_3 \\
&= 586y_1^2 + 869y_1y_2 + 772y_2^2 + 507y_1y_3 + 89y_2y_3 + 423y_3^2
\end{aligned}$$

v_1 und v_2 bilden den öffentlichen Schlüssel. Die Formenmatrizen lauten

$$C_1 = \begin{pmatrix} 515 & 94 & 519 \\ 94 & 253 & 831 \\ 519 & 831 & 797 \end{pmatrix}, \qquad C_2 = \begin{pmatrix} 378 & 380 & 509 \\ 380 & 134 & 158 \\ 509 & 158 & 697 \end{pmatrix}.$$

In der ursprünglichen Basis $\{u_1u_2, u_2u_3, u_3u_1\}$ war es leicht, ein gegebenes quadratisches Polynom als algebraischen Ausdruck in den Basiselementen darzustellen. In der Basis, die aus den Transformationen hervorgeht, ist dies ohne Kenntnis der Transformationen schwierig.

4.3 Unterschreiben einer Nachricht

Die zu signierende Nachricht wird durch $k-1$ Stützstellen $h_1(m), \ldots, h_{k-1}(m)$ repräsentiert. Eine Unterschrift besteht aus Wertzuweisungen an Elemente der Ausgangsbasis G. Im Fall der symmetrischen Basis sind dies die Elemente $\{y_1y_2, y_2y_3, \ldots, y_ky_1\}$. Wegen der Basiseigenschaft von G liegen damit die Werte für alle Polynome aus $F_2[y_1, \ldots, y_k]$ fest. Eine Wertzuweisung, die zur Erfüllung der $k-1$ Kongruenzen

$$\sum_{j,l} (C_i)_{j,l}\, y_j y_l = h_i(m), \quad 1 \le i \le k-1.$$

führt, bildet eine gültige Unterschrift.

Um eine Nachricht zu unterschreiben, wird zunächst der Wert des nicht-veröffentlichten Polynoms $v_k(y_1, \ldots, y_k)$ zufällig gewählt. Durch Invertieren der Matrix B werden die Werte der Polynome transformiert.

$$B^{-1} \cdot \begin{pmatrix} v_1 \\ \vdots \\ v_k \end{pmatrix} = \begin{pmatrix} g_1 \\ \vdots \\ g_k \end{pmatrix}$$

Im Fall der symmetrischen Basis bedeutet das

$$B^{-1} \cdot \begin{pmatrix} v_1 \\ \vdots \\ v_k \end{pmatrix} = \begin{pmatrix} u_1 u_2 \\ \vdots \\ u_1 u_k \end{pmatrix}$$

Da $g_1, \ldots, g_k$ eine algebraische Basis von $F_2[u_1, \ldots, u_k]$ ist, stehen die Werte für die Terme $u_i u_j$, $1 \leq i, j \leq k$ fest.

Die Umkehrung der durchgeführten Variablentransformation lautet

$$\begin{pmatrix} y_1 \\ \vdots \\ y_k \end{pmatrix} = A^{-1} \cdot \begin{pmatrix} u_1 \\ \vdots \\ u_k \end{pmatrix}$$

Jeder Term vom Grad 2 in den neuen Variablen ist eine Summe von Monomen vom Grad 2 in den ursprünglichen Variablen:

$$y_i y_j = (\sum_{l=1}^{k} (a^{-1})_{il} \cdot u_l)(\sum_{l=1}^{k} (a^{-1})_{jl} \cdot u_l), \quad 1 \leq i, j \leq k$$

Die Werte für die Terme vom Grad 2 in den ursprünglichen Variablen sind bekannt. Es stehen damit die Werte für alle Terme vom Grad 2 in den neuen Variablen fest. Die Werte für die Basiselemente $y_1 y_2, \ldots, y_k y_1$ bilden die Unterschrift für die Nachricht m.

Fortsetzung des Beispiels Die Werte, die sich durch Anwendung der Hashfunktionen auf die Nachricht m ergeben, seien $h_1(m) = 786$, $h_2(m) = 348$. Der zufällige Wert für $v_3(y_1, \ldots, y_k)$ sei 569. Es gilt also

$$\begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix} = \begin{pmatrix} 786 \\ 348 \\ 569 \end{pmatrix}$$

Die Inversen der Matrizen A, B lauten

$$A^{-1} = \begin{pmatrix} 627 & 183 & 178 \\ 614 & 466 & 272 \\ 753 & 37 & 759 \end{pmatrix}, \quad B^{-1} = \begin{pmatrix} 318 & 605 & 462 \\ 534 & 214 & 590 \\ 278 & 809 & 387 \end{pmatrix}.$$

Daraus folgt

$$\begin{pmatrix} g_1 \\ g_2 \\ g_3 \end{pmatrix} = \begin{pmatrix} u_1u_2 \\ u_2u_3 \\ u_3u_1 \end{pmatrix} = B^{-1} \cdot \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix} = \begin{pmatrix} 570 \\ 129 \\ 144 \end{pmatrix}$$

und

$$\begin{aligned} u_1^2 &= \frac{(u_1u_2)(u_2u_3)}{(u_2u_3)} = 699, \\ u_2^2 &= \frac{(u_1u_2)(u_2u_3)}{(u_3u_1)} = 623, \\ u_3^2 &= \frac{(u_2u_3)(u_3u_1)}{(u_1u_2)} = 184. \end{aligned}$$

Die Werte für die transformierten Variablen sind

$$\begin{aligned} y_1y_2 &= (627u_1 + 183u_2 + 178u_3)(614u_1 + 466u_2 + 272u_3) = 223, \\ y_2y_3 &= (614u_1 + 466u_2 + 272u_3)(753u_1 + 37u_2 + 759u_3) = 131, \\ y_3y_1 &= (753u_1 + 37u_2 + 759u_3)(627u_1 + 183u_2 + 178u_3) = 516. \end{aligned}$$

Bei der Wertzuweisung $(223, 131, 516)^T$ an die Basiselemente y_1y_2, y_2y_3, y_3y_1 stimmen die Polynome des öffentlichen Schlüssels mit den Stützstellen überein. Es liegt eine gültige Unterschrift vor. □

4.4 Zwei Eigenschaften des Kryptosystems

Die erste Aussage betrifft eine Normierung der Variablentransformation.

Lemma 4.7 Gegeben sei das Signaturschema bezüglich einer Basis, für die jedes Element ein Term vom Grad 2 ist. A und B seien invertierbare Matrizen aus $\mathbb{Z}_n^{k,k}$, so daß $a_{11}, a_{21}, \ldots, a_{k1}$ in $\mathbb{Z}_n$ invertierbar sind.

Dann gibt es invertierbare Matrizen $A', B' \in \mathbb{Z}_n^{k,k}$ mit $a'_{11} = a'_{21} = \ldots = a'_{k1} = 1$, so daß das Paar (A', B') den gleichen öffentlichen Schlüssel wie das Paar (A, B) erzeugt.

Beweis Wir zeigen die Aussage für die symmetrische Basis. Der Beweis für die anderen Basen erfolgt in gleicher Weise.

Sei A' dadurch definiert, daß die i-te Zeile von A mit dem Faktor $a_{i,1}^{-1}$ multipliziert wird, $1 \le i \le k$. Sei B' dadurch definiert, daß die j-te Spalte von B mit dem Faktor $a_{j,1}a_{j+1,1}$ multipliziert wird, $1 \le j \le k$.

Seien $v_1, \ldots, v_k$ die Polynome, die gemäß (4.1) und (4.2) von A und B generiert werden. Seien $v'_1, \ldots, v'_k$ die Polynome, die von A' und B' generiert werden. Es gilt für $1 \le i \le k$:

$$v'_i = \sum_j b'_{ij} \, (\sum_l a'_{jl}y_l) \, (\sum_m a'_{j+1,m}y_m)$$

$$\begin{aligned} &= \sum_j a_{j,1}\, a_{j+1,1}\, b_{ij}\, \frac{1}{a_{j,1}} (\sum_l a_{jl} y_l)\, \frac{1}{a_{j+1,1}} (\sum_m a_{j+1,m} y_m) \\ &= \sum_j b_{ij}\, (\sum_l a_{jl} y_l)\, (\sum_m a_{j+1,m} y_m) \\ &= v_i. \end{aligned}$$

Die Behauptung folgt aus der Definition des öffentlichen Schlüssels nach (4.4). □

In der folgenden Eigenschaft kommt eine Besonderheit der symmetrischen Basis zum Ausdruck. Die Aussage kann leicht verifiziert werden.

Lemma 4.8 Das Matrizenpaar $(A, B) \in (\mathbb{Z}_n^{k,k})^2$ bilde den geheimen Schlüssel bezüglich der symmetrischen Basis.

1. Sei $j \in \{1, \ldots, k\}$. Die Matrix A' entstehe dadurch, daß die Zeilen von A zyklisch um j Zeilen nach unten rotiert werden. Die Matrix B' entstehe dadurch, daß die Spalten von B zyklisch um j Spalten nach rechts rotiert werden.

Es gilt: Das Matrizenpaar (A', B') erzeugt den gleichen öffentlichen Schlüssel wie das Paar (A, B).

2. Die Matrix A' entstehe dadurch, daß die Zeilen von A in entgegengesetzter Reihenfolge angeordnet werden. Die Matrix B' entstehe dadurch, daß die Spalten von B in entgegengesetzter Reihenfolge angeordnet werden.

Es gilt: Das Matrizenpaar (A', B') erzeugt den gleichen öffentlichen Schlüssel wie das Paar (A, B).

Kapitel 5

Der Angriff auf die symmetrische Basis

In diesem Kapitel werden die Ideen der Arbeit von Coppersmith, Stern und Vaudenay (1993) ausgeführt.

5.1 Mathematische Hilfsmittel

5.1.1 Minoren

Definition 5.1 (siehe Gantmacher (1986)) Sei A eine $m \times n$-Matrix. Für $1 \leq i_1 < i_2 < \ldots < i_p \leq m$ und $1 \leq j_1 < j_2 < \ldots < j_p \leq n$ heißt die Determinante

$$\det \begin{pmatrix} a_{i_1 j_1} & a_{i_1 j_2} & \ldots & a_{i_1 j_p} \\ a_{i_2 j_1} & a_{i_2 j_2} & \ldots & a_{i_2 j_p} \\ \vdots & \vdots & \ddots & \vdots \\ a_{i_p j_1} & a_{i_p j_2} & \ldots & a_{i_p j_p} \end{pmatrix}$$

ein **Minor** (oder eine **Unterdeterminante**) **p-ter Ordnung** der Matrix A. Die Matrix A besitzt $\binom{m}{p} \cdot \binom{n}{p}$ Minoren p-ter Ordnung.

Fakt 5.2 (siehe Gantmacher (1986)) Sei $A \neq 0$ eine $m \times n$-Matrix mit Koeffizienten aus einem Körper K. Sei r die größte Ordnung, für die es einen von Null verschiedenen Minor von A gibt. Dann gilt

$$r = \text{Rang}(A).$$

5.1.2 Zeilen- und Spaltenraum einer Formenmatrix

Satz 5.3 Sei K ein Körper mit von zwei verschiedener Charakteristik. Seien $f(y_1, \ldots, y_k)$, $g(y_1, \ldots, y_k)$ homogene lineare Funktionen aus $K[y_1, \ldots, y_k]$, d.h.

$$f(y_1, \ldots, y_k) = \sum_{i=1}^{k} a_i y_i, \quad g(y_1, \ldots, y_k) = \sum_{j=1}^{k} b_j y_j.$$

Für die Formenmatrix Q der homogenen quadratischen Form

$$f(y_1, \ldots, y_k) \cdot g(y_1, \ldots, y_k)$$

gilt: Der Zeilenraum der Matrix Q wird von $(a_1, \ldots, a_k)$ und $(b_1, \ldots, b_k)$ aufgespannt. Der Spaltenraum der Matrix Q wird von $(a_1, \ldots, a_k)^T$ und $(b_1, \ldots, b_k)^T$ aufgespannt.

Beweis Die Matrix Q lautet nach (3.1):

$$Q = \begin{pmatrix} a_1 b_1 & \frac{1}{2}(a_2 b_1 + a_1 b_2) & \cdots & \frac{1}{2}(a_k b_1 + a_1 b_k) \\ \frac{1}{2}(a_1 b_2 + a_2 b_1) & \ddots & & \frac{1}{2}(a_k b_2 + a_2 b_k) \\ \vdots & & & \vdots \\ \frac{1}{2}(a_1 b_k + a_k b_1) & & \cdots & a_k b_k \end{pmatrix}.$$

Sei $l \in \{1, \ldots, k\}$. Die Linearkombination

$$\frac{1}{2} b_l (a_1, \ldots, a_k) + \frac{1}{2} a_l (b_1, \ldots, b_k)$$

der beiden Vektoren $(a_1, \ldots, a_k)$ und $(b_1, \ldots, b_k)$ erzeugt die l-te Zeile von Q, denn

$$\begin{aligned} & \frac{1}{2} b_l (a_1, \ldots, a_k) + \frac{1}{2} a_l (b_1, \ldots, b_k) \\ = \; & (\frac{1}{2} a_1 b_l + \frac{1}{2} a_l b_1, \frac{1}{2} a_2 b_l + \frac{1}{2} a_l b_2, \ldots, \frac{1}{2} a_k b_l + \frac{1}{2} a_l b_k) \\ = \; & l\text{-te Zeile von } Q. \end{aligned}$$

Die Formenmatrix Q ist symmetrisch. Die Aussage für den Spaltenraum folgt deshalb in gleicher Weise. □

5.1.3 Resultanten

Definition 5.4 Sei R ein Integritätsring und R^* die Menge der invertierbaren Elemente von R.

1. Zwei Elemente a und b von R heißen **assoziiert**, wenn es ein $u \in R^*$ mit $a = bu$ gibt.

2. R heißt **faktorieller Ring**, wenn die folgenden beiden Bedingungen erfüllt sind:

(a) Zu jedem $a \in R$ mit $a \neq 0$ und $a \notin R^*$ gibt es irreduzible Elemente $q_1, \ldots, q_r \in R$ mit $a = q_1 \cdot \ldots \cdot q_r$.

(b) Sind $p_1, \ldots, p_r$ und $q_1, \ldots, q_s$ irreduzible Elemente von R mit $p_1 \cdot \ldots \cdot p_r = q_1 \cdot \ldots \cdot q_s$, so gilt $r = s$, und es gibt eine Permutation π der Menge $\{1, \ldots, r\}$, so daß für jedes $i \in \{1, \ldots r\}$ die Elemente p_i und $q_{\pi(i)}$ assoziiert sind.

Für jeden Körper K gilt (siehe z.B. Becker und Weispfennig (1993), Corollary 2.67): $K[x_1, \ldots, x_n]$ ist ein faktorieller Ring, $n \in \mathbb{N}$.

Die Zerlegung von Polynomen aus $K[x_1, \ldots, x_n]$ in irreduzible Elemente ist also eindeutig bis auf Reihenfolge und Einheiten. Diese Tatsache erhebt die Frage nach notwendigen und hinreichenden Kriterien für gemeinsame Faktoren.

Definition 5.5 (siehe Cox, Little, O'Shea (1992), Paragraph 3.6) K sei ein beliebiger Körper. f und g seien aus $K[x_1, \ldots, x_n]$ und haben die Darstellung

$$\begin{aligned} f(x) &= \sum_{i=0}^{m} a_i x_1^i, \quad a_m \neq 0, \\ g(x) &= \sum_{j=0}^{n} b_j x_1^j, \quad b_n \neq 0, \end{aligned}$$

wobei die a_i und die b_j aus $K[x_2, \ldots, x_n]$ stammen. Unter der **Resultante von f und g bezüglich** x_1 versteht man die Determinante

$$\mathrm{Res}(f, g, x_1) = \det \begin{pmatrix} a_0 & a_1 & a_2 & \ldots & a_m & & & \\ & a_0 & a_1 & a_2 & \ldots & a_m & & \\ & & \ddots & \ddots & \ddots & \ldots & \ddots & \\ & & & a_0 & a_1 & a_2 & \ldots & a_m \\ b_0 & b_1 & b_2 & \ldots & b_n & & & \\ & b_0 & b_1 & b_2 & \ldots & b_n & & \\ & & \ddots & \ddots & \ddots & \ldots & \ddots & \\ & & & b_0 & b_1 & b_2 & \ldots & b_n \end{pmatrix} \begin{matrix} \left.\vphantom{\begin{matrix} a \\ a \\ a \\ a \end{matrix}}\right\} n \text{ Zeilen} \\ \left.\vphantom{\begin{matrix} a \\ a \\ a \\ a \end{matrix}}\right\} m \text{ Zeilen} \end{matrix}$$

Die Bedeutung der Resultanten ergibt sich aus dem folgenden Satz (Cox, Little, O'Shea (1992), Paragraph 3.6, Proposition 1):

Satz 5.6 Seien $f, g \in K[x_1, \ldots, x_n]$ mit positivem Grad in x_1. Dann gilt: $\mathrm{Res}(f, g, x_1)$ ist genau dann Null, wenn f und g einen gemeinsamen Faktor in $K[x_1, \ldots, x_n]$ haben, der positiven Grad in x_1 hat.

5.2 Idee des Angriffs

Zunächst soll der allgemeine Rahmen der durchzuführenden Angriffe beschrieben werden. Wir betrachten insbesondere den Fall $k = 5$.

Die Vorgehensweise ist ähnlich wie bei dem Angriff auf das Schema der sequentiellen Linearisierung. Wir analysieren Linearkombinationen der Polynome des öffentlichen Schlüssels in den ursprünglichen Variablen. Es werden Invarianten quadratischer Formen ausgenutzt, die bei Variablentransformationen erhalten bleiben.

Die Formenmatrix eines Polynoms des öffentlichen Schlüssels in den ursprünglichen Variablen hat nur wenige von Null verschiedene Einträge. Im Fall $k = 5$ und der symmetrischen Basis $\{u_1u_2, \ldots, u_ku_1\}$ können nur die zehn Komponenten $(1,2), (2,1), (2,3), (3,2), (3,4), (4,3), (4,5), (5,4), (5,1), (1,5)$ ungleich Null sein. Im nachstehenden Schaubild steht ein Punkt für eine Null und ein Stern für einen beliebigen Eintrag:

$$\begin{pmatrix} \cdot & \star & \cdot & \cdot & \star \\ \star & \cdot & \star & \cdot & \cdot \\ \cdot & \star & \cdot & \star & \cdot \\ \cdot & \cdot & \star & \cdot & \star \\ \star & \cdot & \cdot & \star & \cdot \end{pmatrix}$$

Einige Linearkombinationen der Polynome des öffentlichen Schlüssels bilden quadratische Formen kleinen Ranges. Die zugehörigen Formenmatrizen in den neuen Variablen stehen in engem Zusammenhang zu der durchgeführten Variablentransformation. Wir erhalten dadurch Informationen über die geheime Variablentransformation. Danach werden Informationen über die zweite geheime Transformation ermittelt. Der geheime Schlüssel wird nicht gefunden. Es können aber Unterschriften zu einer vorgegebenen Nachricht generiert werden.

5.3 Fälschen einer Unterschrift

Zunächst wird ein primer Modul n betrachtet. Für den Angriff seien die folgenden Voraussetzungen erfüllt.

Nicht-Entartungsbedingungen 5.7

1. Im Verlauf des Angriffs werden ein k-dimensionaler Vektorraum V sowie Teilräume U_i und T konstruiert. U_i ist ein zweidimensionaler Unterraum von V und T ein $(k-2)$-dimensionaler affiner Teilraum von V.
   Forderung: $U_i \cap T$ sei von der Dimension Null.

2. Im Verlauf des Angriffs wird ein Gleichungssystem in den Variablen $\delta, \epsilon_3, \ldots, \epsilon_{k-1}$ konstruiert. Es wird ein Verfahren angegeben, mit dem $\epsilon_3, \ldots, \epsilon_{k-1}$ in Abhängigkeit von δ ausgedrückt werden können und mit dem ein Polynom vom Grad k in δ

berechnet werden kann.
Forderung: Das Verfahren führe zum Erfolg.

3. Im Verlauf des Angriffs werden Koeffizienten α_i und β_i aus $\mathbb{Z}_n$ verwendet.
Forderung: α_i und β_i seien ungleich Null.

4. Sei A die Variablentransformation des geheimen Schlüssels.
Forderung: In der ersten Spalte von A seien alle Einträge von Null verschieden.

5. Im Verlauf des Angriffs wird die Abhängigkeit eines Koeffizienten δ_2 von einem Koeffizienten δ_1 durch algebraische Bedingungen beschrieben. Wir geben ein Verfahren an, mit dem aus diesen Bedingungen eine quadratische Gleichung in δ_2 in Abhängigkeit von δ_1 konstruiert werden kann.
Forderung: Das Verfahren führe zum Erfolg.

6. Im Verlauf des Angriffs werden algebraische Strukturen konstruiert, die die meisten Eigenschaften einer Körpererweiterung erfüllen.
Forderung: Alle betrachteten Elemente dieser Strukturen seien invertierbar.

7. Im Verlauf des Verfahrens werden lineare Gleichungssysteme aufgestellt, von denen nicht bekannt ist, ob sie regulär sind.
Forderung: Die Gleichungssysteme seien regulär.

5.3.1 Struktur der Formenmatrizen

Sei $i \in \{1, \ldots, k\}$. Das Element $u_i u_{i+1}$ der symmetrischen Basis $\{u_1u_2, \ldots, u_ku_1\}$ ist eine quadratische Form. Die nach (3.1) zugeordnete Formenmatrix hat nur in den beiden Komponenten $(i, i+1)$ und $(i+1, i)$ nichtverschwindende Einträge.

Lemma 5.8 Sei $k \geq 5$. Eine Linearkombination der Basiselemente $u_1u_2, u_2u_3 \ldots, u_ku_1$ ist genau dann eine quadratische Form vom Rang kleiner oder gleich 2, wenn sie von der Form

$$\alpha_i u_{i-1} u_i + \beta_i u_i u_{i+1} \tag{5.1}$$

mit $\alpha_i, \beta_i \in \mathbb{Z}_n$, $1 \leq i \leq k$, ist.

Beweis Sei

$$\sum_{i=1}^{k} a_i \, u_i u_{i+1}, \quad a_1, \ldots, a_k \in \mathbb{Z}_n \tag{5.2}$$

eine Linearkombination der Basiselemente und Q die zugeordnete Formenmatrix.

Die Matrix Q lautet (zur besseren Übersicht werden nur die Einträge aufgeführt, die von Null verschieden sein können)

$$Q = \frac{1}{2}\begin{pmatrix} & a_1 & & & & & a_k \\ a_1 & & a_2 & & & & \\ & a_2 & & a_3 & & & \\ & & a_3 & & \ddots & & \\ & & & \ddots & & a_{k-1} & \\ a_k & & & & a_{k-1} & & \end{pmatrix}.$$

"$\Longleftarrow$" Die Linearkombination (5.2) sei von der Form (5.1). Wegen der Symmetrie der Basiselemente kann o.B.d.A. $i = 2$ in (5.1) angenommen werden. Die Matrix Q lautet

$$Q = \begin{pmatrix} & a_1 & & & & 0 \\ a_1 & & a_2 & & & \\ & a_2 & & 0 & & \\ & & 0 & & \ddots & \\ & & & \ddots & & 0 \\ 0 & & & & 0 & \end{pmatrix}.$$

Der Rang dieser Matrix ist kleiner oder gleich 2.

"$\Longrightarrow$" **Annahme:** Die Linearkombination (5.2) sei nicht von der Form (5.1).

Aufgrund der Symmetrie der Basiselemente genügt es, die Aussage für zwei Fälle zu beweisen.

Fall 1: In (5.2) gilt für alle $i \in \{1, \ldots, k\}$, daß $a_i \neq 0$.

Wegen $k \geq 5$ lautet die linke obere 4×4-Untermatrix von Q:

$$\frac{1}{2}\begin{pmatrix} 0 & a_1 & 0 & 0 \\ a_1 & 0 & a_2 & 0 \\ 0 & a_2 & 0 & a_3 \\ 0 & 0 & a_3 & 0 \end{pmatrix}.$$

Die Untermatrix

$$\frac{1}{2}\begin{pmatrix} 0 & a_1 & 0 \\ a_1 & 0 & 0 \\ 0 & a_2 & a_3 \end{pmatrix}$$

hat Determinante $-(\frac{1}{2})^3 a_1^2 a_3 \neq 0$. Mit Fakt 5.2 folgt $\mathrm{Rang}(Q) \geq 3$.

Fall 2: In (5.2) gibt es ein $j \in \{3, \ldots, k-1\}$, so daß $a_1 \neq 0$, $a_2 = \ldots = a_{j-1} = 0$, $a_j \neq 0$.

Die linke obere $(j+1) \times (j+1)$-Untermatrix von Q lautet

$$\frac{1}{2}\begin{pmatrix} & a_1 & & & & x \\ a_1 & & 0 & & & \\ & 0 & & \ddots & & \\ & & \ddots & & 0 & \\ & & & 0 & & a_j \\ x & & & & a_j & \end{pmatrix} \quad \text{mit } x := \begin{cases} 0, & \text{wenn } j < k-1 \\ a_k, & \text{wenn } j = k-1 \end{cases}.$$

Die Untermatrix

$$\frac{1}{2}\begin{pmatrix} 0 & a_1 & x \\ a_1 & 0 & 0 \\ 0 & 0 & a_j \end{pmatrix}$$

hat Determinante $-(\frac{1}{2})^3 a_1^2 a_j \neq 0$. Mit Fakt 5.2 folgt $\text{Rang}(Q) \geq 3$. □

Bemerkung 5.9 Im Fall $(\alpha_i, \beta_i) \neq (0,0)$ hat die quadratische Form (5.1) genau den Rang 2.

Lemma 5.10 Für $k \geq 5$ seien $v_1, \ldots, v_{k-1}$ die Polynome des öffentlichen Schlüssels. Dann gilt: Für jedes $i \in \{1, \ldots, k\}$ gibt es genau ein Paar $(\alpha_i, \beta_i) \in \mathbb{Z}_n^2$ und genau ein Tupel von Koeffizienten $(\delta_i, \epsilon_{3,i}, \ldots, \epsilon_{k-1,i}) \in \mathbb{Z}_n^{k-2}$, so daß

$$\alpha_i u_{i-1} u_i + \beta_i u_i u_{i+1} = v_1 + \delta_i v_2 + \sum_{3 \leq j \leq k-1} \epsilon_{j,i} v_j. \tag{5.3}$$

Beweis Betrachte den linearen Raum V der Linearkombinationen $\sum_{i=1}^{k} a_i \; u_i u_{i+1}$ für beliebige $a_i \in \mathbb{Z}_n$, $1 \leq i \leq k$. Der Vektorraum V hat Dimension k.

Die Linearkombinationen $\alpha_i u_{i-1} u_i + \beta_i u_i u_{i+1}$ für beliebige $\alpha_i, \beta_i \in \mathbb{Z}_n$ bilden einen zweidimensionalen Unterraum U_i von V.

Die Formen $v_1 + \delta v_2 + \sum_{3 \leq j \leq k-1} \epsilon_j v_j$ mit beliebigen Koeffizienten $\delta, \epsilon_3, \ldots, \epsilon_{k-1} \in \mathbb{Z}_n$ bilden einen Unterraum T der Dimension kleiner oder gleich $k-2$ von V. Die quadratischen Formen $v_1, \ldots, v_{k-1}$ sind linear unabhängig, weil die Matrix B aus (4.2) regulär ist. Damit gilt $\dim T = k-2$. Im nicht-entarteten Fall gemäß Forderung 1 ist $U_i \cap T$ von der Dimension Null. □

Bemerkung 5.11 Die quadratische Form aus (5.3) hat nach Lemma 5.8 den Rang kleiner oder gleich 2. Da die Transformationsmatrix B aus (4.2) regulär ist, kann die Summe auf der rechten Seite von (5.3) nicht das Nullpolynom erzeugen. Aus Bemerkung 5.9 folgt damit, daß die quadratische Form aus (5.3) *genau* vom Rang 2 ist.

Das Lemma 5.10 hat eine zentrale Bedeutung. Die Bezeichnungen α_i, β_i, δ_i, $\epsilon_{3,i}, \ldots, \epsilon_{k-1,i}$, $1 \leq i \leq k$, sollen im folgenden wie in Lemma 5.10 definiert sein.

Von nun an wird nur noch der Fall $k = 5$ betrachtet. In Abschnitt 5.6 wird auf andere Werte für k eingegangen.

5.3.2 Elimination der Koeffizienten

Bezeichnung 5.12 Seien $v_1, \ldots, v_{k-1}$ die durch (4.2) definierten Polynome des öffentlichen Schlüssels. Dann bezeichnet $\tau(\delta, \epsilon_3, \ldots, \epsilon_{k-1})$ die Formenmatrix von

$$v_1 + \delta v_2 + \sum_{3 \le j \le k-1} \epsilon_j v_j$$

in den neuen Variablen $y_1, \ldots, y_k$.

Der Rang der Matrix τ ist nach Fakt 5.2 genau dann höchstens 2, wenn jeder Minor dritter Ordnung 3 von τ verschwindet. Im Fall $k = 5$ gibt es

$$\binom{5}{3} \cdot \binom{5}{3} = 10 \cdot 10 = 100$$

Minoren dritter Ordnung. Unter Berücksichtigung der Symmetrie von τ können davon maximal

$$\frac{1}{2}\binom{5}{3}\binom{5}{3} + \frac{1}{2}\binom{5}{3} = 50 + 5 = 55$$

verschieden sein. Das Verschwinden eines Minors dritter Ordnung von $\tau(\delta, \epsilon_3, \epsilon_4)$ kann als Polynomgleichung der Form

$$\sum_{0 \le i,j,l \le 3,\ i+j+l \le 3} \lambda_{ijl} \cdot \delta^i \epsilon_3^j \epsilon_4^l = 0 \quad \text{mit} \quad \lambda_{ijl} \in \mathbb{Z}_n,\ 1 \le i,j,l \le 3,\ i+j+l \le 3 \tag{5.4}$$

geschrieben werden.

Jedes Polynom auf der linken Seite einer Gleichung besteht aus maximal 20 Monomen. Wir interpretieren jeden Term $\delta^i \epsilon_3^j \epsilon_4^l$, $0 \le i,j,l \le 3$, $i+j+l \le 3$ als Unbekannte eines aus 55 Gleichungen bestehenden linearen Gleichungssystems in 20 Unbestimmten. Wie beim Gauß-Algorithmus für lineare Gleichungssysteme werden Terme eliminiert, indem Vielfache einer Gleichung von den anderen Gleichungen subtrahiert werden:

1. Eliminiere alle Monome, in denen ϵ_3 auftritt bis auf $\delta^0 \epsilon_3^1 \epsilon_4^0 = \epsilon_3$. Dies liefert ein Polynom $\epsilon_3(\delta, \epsilon_4) \in \mathbb{Z}_n[\delta, \epsilon_4]$. Setze $\epsilon_3(\delta, \epsilon_4)$ in (5.4) ein.

2. Eliminiere alle Monome, in denen ϵ_4 auftritt bis auf $\delta^0 \epsilon_3^0 \epsilon_4^1 = \epsilon_4$. Dies liefert ein Polynom $\epsilon_4(\delta) \in \mathbb{Z}_n[\delta]$. Setze $\epsilon_4(\delta)$ in (5.4) ein.

3. Nach der Elimination von ϵ_3 und ϵ_4 ist (5.4) in Polynomgleichungen in δ übergeführt. Sei $P(\delta)$ der größte gemeinsame Teiler der Polynome, die auf der linken Seite der Gleichungen stehen.

4. Setze $\epsilon_4(\delta)$ in $\epsilon_3(\delta, \epsilon_4)$ ein. Dies liefert ein Polynom $\epsilon_3(\delta) \in \mathbb{Z}_n[\delta]$.

Nach Lemma 5.8 und Lemma 5.10 gibt es genau $k = 5$ verschiedene Tupel $(\delta_i, \epsilon_{3,i}, \epsilon_{4,i})$, $1 \le i \le 5$, für die das Gleichungssystem (5.4) erfüllt wird. Für die Polynome $\epsilon_3(\delta)$, $\epsilon_4(\delta)$ und $P(\delta)$ gilt deshalb:

- $\delta_1, \ldots, \delta_5$ sind Nullstellen von $P(\delta)$. $P(\delta)$ hat keine weiteren Nullstellen.
- $(\delta_i, \epsilon_3(\delta_i), \epsilon_4(\delta_i)) = (\delta_i, \epsilon_{3,i}, \epsilon_{4,i}), \quad 1 \leq i \leq 5.$

Bemerkung 5.13 Im nicht-entarteten Fall gemäß Forderung 2 gilt:

- $\delta_1, \ldots, \delta_5$ sind paarweise verschieden.
- $\delta_1, \ldots, \delta_5$ sind einfache Nullstellen von $P(\delta)$.
- Das Polynom $P(\delta)$ hat *genau* den Grad $k = 5$.

5.3.3 Charakterisierung der Variablentransformation

Sei $P(\delta)$ das Polynom vom Grad k mit den durch Lemma 5.10 bestimmten Nullstellen $\delta_1, \ldots, \delta_k$. Die k verschiedenen Nullstellen von $P(\delta)$ werden durch algebraische Bedingungen unterschieden.

Betrachte die in Bezeichnung 5.12 eingeführte Formenmatrix $\tau = \tau(\delta, \epsilon_3, \ldots, \epsilon_{k-1})$ von

$$v_1 + \delta v_2 + \sum_{3 \leq j \leq k-1} \epsilon_j v_j$$

in den neuen Variablen. Seien $(\delta_i, \epsilon_{3,i}, \ldots, \epsilon_{k-1,i})$ wie in Lemma 5.10 die Koeffiziententupel, für die $\tau(\delta_i, \epsilon_{3,i}, \ldots, \epsilon_{k-1,i})$ einen Rang kleiner oder gleich 2 hat, $1 \leq i \leq k$.

Werden $\epsilon_3, \ldots, \epsilon_{k-1}$ durch die polynomialen Ausdrücke $\epsilon_3(\delta), \ldots, \epsilon_{k-1}(\delta)$ in δ ersetzt, dann ist die Matrix τ eine Matrix $\tau(\delta)$ in Abhängigkeit von δ. Für jede (unbekannte) Nullstelle δ_i von $P(\delta)$ ist $\tau(\delta_i)$ nach Bemerkung 5.11 eine Matrix vom Rang 2.

Bezeichnung 5.14 Sei Y_i der Spaltenraum von $\tau(\delta)$ an der Stelle $\delta = \delta_i$.

Y_i ist ein Unterraum von $\mathbb{Z}_n^k$ der Dimension 2, $1 \leq i \leq k$. Die Matrix τ ist symmetrisch. Der Zeilenraum von τ stimmt deshalb mit dem Spaltenraum von τ (bis auf Transponierung der Vektoren) überein.

Bezeichnung 5.15 Beim Generieren eines Schlüsselpaares führt die Matrix A aus (4.1) die ursprünglichen Variablen $u_1, \ldots, u_k$ in die neuen Variablen $y_1, \ldots y_k$ über:

$$u_i = \sum_{j=1}^{k} a_{ij} y_j, \quad 1 \leq i \leq k.$$

Im folgenden bezeichnen wir den Koeffizientenvektor $(a_{i,1}, \ldots, a_{i,k})^T$ ebenfalls mit u_i, $1 \leq i \leq k$. Es geht jeweils aus dem Zusammenhang hervor, ob die Variable u_i oder der Koeffizientenvektor u_i gemeint ist.

Lemma 5.16 Für $k = 5$ seien $Y_1, \ldots, Y_k$ die in Bezeichnung 5.14 eingeführten Spaltenräume und $u_1, \ldots, u_k$ die in Bezeichnung 5.15 eingeführten Koeffizientenvektoren. Die Koeffizienten α_i, β_i seien wie in Lemma 5.10 bestimmt, $1 \leq i \leq k$. Dann gilt:

$$Y_i = \text{span}(u_i, \alpha_i u_{i-1} + \beta_i u_{i+1}), \quad 1 \leq i \leq k.$$

Beweis Y_i ist der Spaltenraum der Formenmatrix von

$$\alpha_i u_i u_{i-1} + \beta_i u_i u_{i+1} = u_i \cdot (\alpha_i u_{i-1} + \beta_i u_{i+1})$$

in den neuen Variablen. Die Aussage folgt aus Satz 5.3. □

Nun kann eine Beziehung für die Koeffizientenvektoren $u_1, \ldots, u_k$ der Variablentransformation aufgestellt werden.

Lemma 5.17 Für $k = 5$ seien $Y_1, \ldots, Y_k$ die in Bezeichnung 5.14 eingeführten Spaltenräume, und $u_1, \ldots, u_k$ die in Bezeichnung 5.15 eingeführten Koeffizientenvektoren. Es gilt

$$\begin{aligned} u_i &\in Y_i \cap (Y_{i+1} + Y_{i+2}) \cap (Y_{i-1} + Y_{i-2}) && (5.5) \\ \text{und } \alpha_i u_{i-1} + \beta_i u_{i+1} &\in Y_i \cap (Y_{i-2} + Y_{i+2}) \cap (Y_{i-1} + Y_{i+1}). && (5.6) \end{aligned}$$

Die durch die Schnittmengen bestimmten Unterräume sind eindimensional.

Beweis Im nicht-entarteten Fall gemäß Forderung 3 sind $\alpha_1, \ldots, \alpha_k$ und $\beta_1, \ldots, \beta_k$ von Null verschieden. Sei $i \in \{1, \ldots, k\}$.

1. (a) $u_i \in Y_i$: Diese Aussage folgt unmittelbar aus der Beziehung

$$Y_i = \text{span}(u_i, \alpha_i u_{i-1} + \beta_i u_{i+1}).$$

(b) $u_i \in Y_{i+1} + Y_{i+2}$: Es gilt

$$Y_{i+1} + Y_{i+2} = \text{span}(u_{i+1}, \alpha_{i+1} u_i + \beta_{i+1} u_{i+2}, u_{i+2}, \alpha_{i+2} u_{i+1} + \beta_{i+2} u_{i+3}). \tag{5.7}$$

Aus den beiden Aussagen

$$\begin{aligned} u_i &\in \text{span}(\alpha_{i+1} u_i + \beta_{i+1} u_{i+2}, u_{i+2}) \\ \text{und } \text{span}(\alpha_{i+1} u_i + \beta_{i+1} u_{i+2}, u_{i+2}) &\subseteq Y_{i+1} + Y_{i+2} \end{aligned}$$

folgt $u_i \in Y_{i+1} + Y_{i+2}$.

(c) Analog wird $u_i \in Y_{i-1} + Y_{i-2}$ gezeigt.

Wir zeigen nun, daß der durch den Schnitt beschriebene Unterraum eindimensional ist. Ein von u_i linear unabhängiger Vektor in Y_i hat die Form

$$a \cdot u_i + b \cdot (\alpha_i u_{i-1} + \beta_i u_{i+1}), \quad a, b \in \mathbb{Z}_n, \quad b \neq 0.$$

Die Vektoren $u_1, \ldots, u_k$ sind die Zeilen der Transformationsmatrix A aus (4.1) und damit linear unabhängig. Es gibt nach (5.7) keinen Vektor in $Y_1 + Y_2$, der diese Form hat.

2. Die Aussage folgt analog zur ersten Aussage aus den Beziehungen

$$\begin{aligned} Y_i &= \operatorname{span}(u_i, \alpha_i u_{i-1} + \beta_i u_{i+1}), \\ Y_{i-2} + Y_{i+2} &= \operatorname{span}(u_{i-2}, \alpha_{i-2} u_{i-3} + \beta_{i-2} u_{i-1}, u_{i+2}, \alpha_{i+2} u_{i+1} + \beta_{i+2} u_{i+3}) \\ &= \operatorname{span}(u_{i-2}, \alpha_{i-2} u_{i+2} + \beta_{i-2} u_{i-1}, u_{i+2}, \alpha_{i+2} u_{i+1} + \beta_{i+2} u_{i-2}), \\ Y_{i-1} + Y_{i+1} &= \operatorname{span}(u_{i-1}, \alpha_{i-1} u_{i-2} + \beta_{i-1} u_i, u_{i+1}, \alpha_{i+1} u_i + \beta_{i+1} u_{i+2}). \end{aligned}$$

□

Die Schnittbedingungen legen die Koeffizientenvektoren $u_1, \ldots, u_k$ nur bis auf konstante Faktoren fest. Im nicht-entarteten Fall gemäß Forderung 4 ist die erste Komponente jedes Koeffizientenvektors ungleich Null. Die Vektoren $u_1, \ldots, u_k$ können deshalb nach nach Lemma 4.7 so normiert werden, daß die erste Komponente 1 ist.

Wir wollen diese algebraischen Bedingungen nun in polynomiale Gleichungssysteme umsetzen.

Umsetzung der algebraischen Bedingungen

Das nachstehende Verfahren liefert Polynomgleichungen in $\delta_1, \ldots, \delta_5$ und polynomiale Ausdrücke für $u_1, \ldots, u_5$. Zunächst soll eine polynomiale Beziehung für u_3 aufgestellt werden.

Wir betrachten die erste Schnittbedingung aus Lemma 5.17 für $i = 3$.

$$u_3 \quad \in \quad Y_3 \cap (Y_1 + Y_2) \cap (Y_4 + Y_5) \qquad \text{(Dimension 1)}$$

Y_i ist der Spaltenraum der Matrix $\tau(\delta_i)$, $1 \le i \le k$. Die Matrix $\tau(\delta_i)$ ist uns in polynomialer Abhängigkeit von δ_i bekannt, $1 \le i \le k$.

$Y_1 + Y_2$ hat die Dimension 4 und wird durch 4 Spaltenvektoren $z_1, \ldots, z_4$ aufgespannt. Y_3 hat die Dimension 2 und wird durch 2 Spaltenvektoren x und y aufgespannt. Seien x und y linear unabhängig von $z_1, \ldots, z_4$. Der Raum $Y_3 \cap (Y_1 + Y_2)$ ist eindimensional. Der Koeffizientenvektor $u_3 \in Y_3 \cap (Y_1 + Y_2)$ hat deshalb eine Darstellung der Form $u_3 = ax + by$ mit Koeffizienten $a, b \in \mathbb{Z}_n$. a und b müssen die folgende Bedingung erfüllen:

$$\begin{aligned} & ax + by \in Y_1 + Y_2 \\ \iff \quad & \det(ax + by, z_1, \ldots, z_4) = 0 \\ \iff \quad & a \cdot \det(x, z_1, \ldots, z_4) + b \cdot \det(y, z_1, \ldots, z_4) = 0. \end{aligned}$$

Wählt man $a = -\det(y, z_1, \ldots, z_4)$, $b = \det(x, z_1, \ldots, z_4)$, so ist diese Bedingung erfüllt. Definiere

$$u_3' := -\det(y, z_1, \ldots, z_4) \cdot x + \det(x, z_1, \ldots, z_4) \cdot y.$$

u_3' unterscheidet sich nur um einen konstanten Faktor von u_3. Nach Lemma 4.7 ist dieser konstante Faktor unbedeutend. Wir können deshalb u_3 und u_3' identifizieren. Später

wird die erste Komponente von u_3 auf 1 normiert. In gleicher Weise können u_1, u_2, u_4, u_5 bestimmt werden.

Man beachte jedoch: Die berechneten Ausdrücke für $u_1, \ldots, u_5$ sind polynomiale Ausdrücke in den uns unbekannten Koeffizienten $\delta_1, \ldots, \delta_5$.

Es werden nun zwei Polynomgleichungen aufgestellt, die die Werte $\delta_1, \ldots, \delta_5$ untereinander in Relation setzen. Betrachte hierzu die beiden algebraischen Bedingungen, die aus Lemma 5.17 folgen:

$$Y_3 \cap (Y_1 + Y_2) \cap (Y_4 + Y_5) \neq 0. \tag{5.8}$$
$$Y_4 \cap (Y_1 + Y_2) \cap (Y_3 + Y_5) \neq 0. \tag{5.9}$$

Der Unterraum $Y_4 + Y_5$ ist vierdimensional. Seien $t_1, \ldots, t_4$ vier Vektoren, die $Y_4 + Y_5$ aufspannen. Sei u der polynomiale Ausdruck für u_3. u wurde mit Hilfe der Bedingung

$$u \in Y_3 \cap (Y_1 + Y_2)$$

berechnet.

Die Bedingung (5.8) läßt sich umformen:

$$\begin{aligned} & Y_3 \cap (Y_1 + Y_2) \cap (Y_4 + Y_5) \neq 0 \\ \iff \quad & u \in Y_4 + Y_5 \\ \iff \quad & \det(u, t_1, \ldots, t_4) = 0 \end{aligned}$$

Die Berechnung der Determinante in Abhängigkeit von $\delta_1, \ldots, \delta_5$ liefert eine Polynomgleichung in $\delta_1, \ldots, \delta_5$.

Die Schnittbedingung (5.6) ergibt analog eine zweite Polynomgleichung in $\delta_1, \ldots, \delta_5$.

Bezeichnung 5.18 Die beiden Polynomgleichungen in $\delta_1, \ldots, \delta_5$ werden mit

$$g_1(\delta_1, \ldots, \delta_5) = 0, \quad g_2(\delta_1, \ldots, \delta_5) = 0$$

bezeichnet.

Die gefundenen Polynome in $\delta_1, \ldots, \delta_5$ sind hochgradig in mehreren Unbestimmten, sie können damit mehrere tausend Terme enthalten. Zwei Gründe machen eine Reduktion der Polynome unabdingbar:

- Der Aufwand beim Umgang mit Polynomen der beschriebenen Größenordnung ist unermeßlich groß.
- Um die Polynome sinnvoll verarbeiten zu können, ist eine kanonische Struktur erforderlich.

5.3.4 Reduktion der Polynome

Jeder (uns unbekannte) Wert δ_i ist eine Nullstelle des Polynoms $P(\delta)$, welches den Grad k hat. Damit kann jedes Vorkommen einer Variablen δ_i in einer beliebigen Polynomgleichung auf den Grad $k-1$ reduziert werden. Die auf diese Weise reduzierten Polynome enthalten im Fall $k = 5$ maximal $5^5 = 3125$ Terme. Wir werden die Polynome weiter reduzieren, so daß sie aus maximal $5! = 120$ Termen bestehen.

Nach Bemerkung 5.13 sind $\delta_1, \ldots, \delta_5$ im nicht-entarteten Fall paarweise verschieden. Um zu gewährleisten, daß $\delta_1, \ldots, \delta_5$ verschiedene Nullstellen von $P(\delta)$ sind, definieren wir

$$\begin{aligned} P_2(\delta) &= \frac{P(\delta) - P(\delta_1)}{\delta - \delta_1}, \\ P_3(\delta) &= \frac{P_2(\delta) - P_2(\delta_2)}{\delta - \delta_2}, \\ P_4(\delta) &= \frac{P_3(\delta) - P_3(\delta_3)}{\delta - \delta_3}, \\ P_5(\delta) &= \frac{P_4(\delta) - P_4(\delta_4)}{\delta - \delta_4}. \end{aligned}$$

$\delta_2, \ldots, \delta_5$ sind verschieden von δ_1. Es gilt deshalb

$$P_2(\delta_i) = 0, \quad 2 \leq i \leq 5.$$

$\delta_3, \ldots, \delta_5$ sind verschieden von δ_1 und δ_2. Es gilt

$$P_3(\delta_i) = 0, \quad 3 \leq i \leq 5.$$

Analog folgt

$$\begin{aligned} P_4(\delta_i) &= 0, \quad 4 \leq i \leq 5, \\ P_5(\delta_5) &= 0. \end{aligned}$$

$P_2(\delta_2)$ ist ein Polynom vom Grad 4 in δ_1 und in δ_2. Damit kann jedes Auftreten von δ_2 auf den Grad 3 reduziert werden.

Das Polynom $P_3(\delta_3)$ ist vom Grad 3 in δ_1, δ_2 und δ_3. Jedes Auftreten von δ_3 kann auf den Grad 2 reduziert werden.

Mit Hilfe von $P_4(\delta_4)$ kann jedes Auftreten von δ_4 auf den Grad 1 reduziert werden. $P_5(\delta_5)$ dient zum Eliminieren der Vorkommen von δ_5.

Jeder Term der auf diese Weise reduzierten Polynome hat die Form

$$\delta_1^i \delta_2^j \delta_3^k \delta_4^l \text{ mit}$$

$$0 \leq i \leq 4, \quad 0 \leq j \leq 3, \quad 0 \leq k \leq 2, \quad 0 \leq l \leq 1.$$

Die reduzierten Polynome bestehen damit aus maximal $5 \cdot 4 \cdot 3 \cdot 2 = 120$ Monomen.

5.3.5 Die Symmetrie

Die Bedingungen in Lemma 5.17 für die Räume $Y_1, \ldots, Y_5$ sind symmetrisch in folgendem Sinne: Wenn eine Belegung für $\delta_1, \ldots, \delta_5$ die Bedingungen erfüllt, dann erfüllt auch $\delta'_1, \ldots, \delta'_5$ mit $\delta'_i = \delta_{i+1}$, $1 \leq i \leq 5$, die Bedingungen. $u_1, \ldots, u_5$ gehen in diesem Fall in $u'_1, \ldots, u'_5$ mit $u'_i = u_{i+1}$, $1 \leq i \leq 5$, über. Diese **zyklische Symmetrie** beruht auf der ersten Aussage von Lemma 4.8.

Die zweite Aussage von Lemma 4.8 impliziert eine **Spiegelsymmetrie**: Wenn eine Belegung für $\delta_1, \ldots, \delta_5$ die Bedingungen erfüllt, dann erfüllt auch $\delta'_1, \ldots, \delta'_5$ mit $\delta'_{1+i} = \delta_{1-i}$, $1 \leq i \leq k$, die Bedingungen. $u_1, \ldots, u_5$ gehen in diesem Fall in $u'_1, \ldots, u'_5$ mit $u'_{1+i} = u_{1-i}$, $1 \leq i \leq k$, über.

Wegen Lemma 4.8 ist es nicht möglich, mit Hilfe algebraischer Bedingungen $\delta_1, \ldots, \delta_5$ eindeutig zu bestimmen. Wir werden nun zeigen, daß die beiden beschriebenen Symmetrien die einzigen in dem System sind.

Das nachfolgende Lemma zeigt, daß bei festem δ_1 die Koeffizienten δ_2 und δ_5 von den Koeffizienten δ_3 und δ_4 unterschieden werden können. Es werden dazu die beiden Schnittbedingungen

$$\begin{aligned} Y_j \cap (Y_1 + Y_i) \cap (Y_l + Y_m) &\neq \{0\}. \\ Y_l \cap (Y_1 + Y_i) \cap (Y_j + Y_m) &\neq \{0\}. \end{aligned}$$

aus (5.8) und (5.9) bei noch unbekannter Zuordnung von i, j, l, m zu den Werten 2, 3, 4, 5 betrachtet.

Lemma 5.19 Sei $k = 5$. Für jede bijektive Zuordnung von i, j, l, m zu den Werten 2, 3, 4, 5, die zur Erfüllung der beiden Schnittbedingungen

$$\begin{aligned} Y_j \cap (Y_1 + Y_i) \cap (Y_l + Y_m) &\neq \{0\}. \\ Y_l \cap (Y_1 + Y_i) \cap (Y_j + Y_m) &\neq \{0\}. \end{aligned}$$

führt, gilt $i = 2$ oder $i = 5$.

Beweis Für jede bijektive Zuordnung von i, j, l, m zu den Werten $2, 3, 4, 5$ können die Bedingungen analog zu Lemma 5.17 nachgerechnet werden. □

Das nachstehende Lemma besagt, daß bei festem δ_1 und δ_2 die Koeffizienten δ_3, δ_4 und δ_5 unterschieden werden.

Lemma 5.20 Sei $k \geq 5$, δ_1 und δ_2 seien fest. Durch die Schnittbedingungen aus (5.5) und (5.6)

$$\begin{aligned} Y_i \cap (Y_{i+1} + Y_{i+2}) \cap (Y_{i-1} + Y_{i-2}) &\neq \{0\}, \quad 1 \leq i \leq k, \\ \text{und } Y_i \cap (Y_{i-2} + Y_{i+2}) \cap (Y_{i-1} + Y_{i+1}) &\neq \{0\}, \quad 1 \leq i \leq k, \end{aligned}$$

sind die Räume Y_3, Y_4 und Y_5 eindeutig festgelegt.

Beweis Die Eindeutigkeit von Y_5 ergibt sich aus der Unterscheidung der Räume Y_2, Y_5 von den Räumen Y_3, Y_4 im voranstehenden Lemma. Die Unterscheidung von Y_3 und Y_4 ergibt sich dadurch, daß

$$\begin{aligned} Y_1 \cap (Y_2 + Y_3) &\neq \{0\} \\ Y_1 \cap (Y_2 + Y_4) &= \{0\}. \end{aligned}$$

□

Sei δ_1 fest. Nach Lemma 5.20 zeichnen die algebraischen Bedingungen die beiden Werte δ_2 und δ_5 von den beiden Werten δ_3 und δ_4 aus.

Mit dem folgenden Verfahren wird eine quadratische Gleichung in δ_2 (in Abhängigkeit von δ_1) berechnet, deren zwei Lösungen als δ_2 und als δ_5 dienen können. Nach Forderung 5 der Nicht-Entartungsbedingungen gelingt dies.

5.3.6 Konstruktion der quadratischen Gleichung

Seien $g_1 = 0$, $g_2 = 0$ die in Bezeichnung 5.18 eingeführten Polynomgleichungen nach der Reduktion. Die beiden Gleichungen sind Umsetzungen der algebraischen Bedingungen aus Lemma 5.19, mit denen es möglich ist, δ_2 und δ_5 von δ_3 und δ_4 auszuzeichnen.

Mit den Resultanten

$$\begin{aligned} r_1 &= \mathrm{Res}(g_1, g_2, \delta_3), \\ r_2 &= \mathrm{Res}(P(\delta_4), r_1, \delta_4), \\ r_3 &= \mathrm{Res}(P(\delta_3), r_2, \delta_3) \end{aligned}$$

liegt mit r_3 eine Polynomgleichung vor, in der δ_3 und δ_4 nicht mehr vorkommen. Eine zweite Gleichung dieser Form erhält man mit

$$\begin{aligned} s_1 &= \mathrm{Res}(g_1, P_4(\delta_4), \delta_4), \\ s_2 &= \mathrm{Res}(g_2, P_4(\delta_4), \delta_4), \\ s_3 &= \mathrm{Res}(s_1, s_2, \delta_3). \end{aligned}$$

r_3 und s_3 sind vom Grad kleiner oder gleich 4 in δ_1 und vom Grad kleiner oder gleich 3 in δ_2. Im nicht-entarteten Fall gemäß Forderung 5 sind r_3 und s_3 genau vom Grad 3 in δ_2.

Sei a der Koeffizient von δ_2^3 in r_3 und b der Koeffizient von δ_2^3 in s_3. a und b sind Polynome vierten Grades in δ_1. Die Subtraktion

$$a \cdot s_3 - b \cdot r_3$$

eliminiert den Term δ_2^3. Es entsteht eine quadratische Gleichung in δ_2.

Bezeichnung 5.21 Wir schreiben $\delta_1 = X$ und $\delta_2 = Y$, um anzudeuten, daß δ_1 und δ_2 von nun an fest sein sollen. Die quadratische Gleichung in $\delta_2 = Y$ wird mit $Q(X, Y) = 0$ bezeichnet.

Mit Hilfe der quadratischen Gleichung und den nachstehenden Überlegungen kann ein beliebiges Polynom in den Variablen X und Y so reduziert werden, daß jeder Term die Form

$$X^i Y^j \text{ mit } \quad 0 \leq i \leq 4, \quad 0 \leq j \leq 1$$

hat.

Rechnen modulo des quadratischen Polynoms

Ein Polynom in X, das mit Hilfe des Polynoms $P(X)$ reduziert wird, kann als Restklasse des Polynomrings $K[X]$ (mit $K := \mathbb{Z}_n$) modulo dem von $P(X)$ erzeugten Ideal aufgefaßt werden. Wir schreiben für den Restklassenring $K[X]/P(X)$. Es gilt der folgende Zusammenhang (siehe z.B. Becker und Weispfennig (1993)).

Fakt 5.22 Sei K' ein Körper, $p(x) \in K'[x]$. $K'[x]/p(x)$ ist genau dann ein Körper, wenn $p(x)$ irreduzibel ist.

$P(X)$ ist zwar nicht irreduzibel, aber fast alle Elemente des Restklassenrings $K[X]/P(X)$ sind invertierbar. Wir können den Ring im nicht-entarteten Fall gemäß Forderung 6 näherungsweise als einen Körper betrachten.

Wir interpretieren die Polynome in X und Y als Polynome in Y mit Koeffizienten aus dem Körper $K[X]/P(X)$. Die durch $Q(X,Y)$ reduzierten Polynome können als Restklassen des Polynomrings $(K[X]/P(X))[Y]$ modulo dem von $Q(X,Y)$ erzeugten Ideal aufgefaßt werden. $Q(X,Y)$ ist zwar nicht irreduzibel, aber fast alle Elemente des Restklassenrings $(K[X]/P(X))[Y]/Q(X,Y)$ sind invertierbar. Wir können den Ring für unsere Zwecke wieder näherungsweise als einen Körper betrachten. $(K[X]/P(X))[Y]/Q(X,Y)$ wird also als zweifache Körpererweiterung von K interpretiert.

Für einen beliebigen Körper K' ist $K'[x]$ ein Euklidischer Ring (siehe z.B. Becker und Weispfennig (1993), Proposition 2.24). $(K[X]/P(X))[Y]$ ist deshalb ein Euklidischer Ring. Das Invertieren von Elementen in $(K[X]/P(X))[Y]/Q(X,Y)$ mit dem Euklidischen Algorithmus erfordert Invertierungen im Grundkörper $(K[X]/P(X))$. Zum Berechnen inverser Elemente in diesem Grundkörper dient wiederum der Euklidische Algorithmus.

Von nun an werden alle Rechnungen im Restklassenring $(K[X]/P(X))[Y]/Q(X,Y)$ durchgeführt.

Ziel ist es, Ausdrücke für $\delta_3, \ldots, \delta_5$ in Abhängigkeit von X und Y zu ermitteln. Wegen der Symmetrie wird die quadratische Gleichung $Q(\delta_2, \delta) = 0$ von δ_3 und von δ_1 gelöst. δ_3 ist die von δ_1 verschiedene Nullstelle dieser quadratischen Gleichung in δ. Deshalb ist δ_3 eine Nullstelle des folgenden Polynoms in δ:

$$\frac{Q(Y,\delta) - Q(X,Y)}{\delta - X}$$

Dieses Polynom ist linear in δ.

Wir können damit δ_3 als Polynom in X und Y ausdrücken. Auf gleiche Weise entstehen Ausdrücke für δ_4 und δ_5 in Abhängigkeit von X und Y. Damit läßt sich jedes Polynom in $\delta_1, \ldots, \delta_5$ auf ein Polynom in X und Y transformieren. Dieses hat maximal den Grad 4 in X und den Grad 1 in Y.

Die Einträge der Koeffizientenvektoren $u_1, \ldots, u_5$ stammen aus der zweifachen Körpererweiterung. Da Elemente aus dieser Menge im nicht-entarteten Fall invertierbar sind, können die Koeffizientenvektoren $u_1, \ldots, u_5$ gemäß den Ausführungen nach Lemma 5.17 so normiert werden, daß die erste Komponente 1 ist.

5.3.7 Substitution des Signaturprotokolls

Die linearen Funktionen, die die Variablen $u_1, \ldots, u_k$ in die Variablen $y_1, \ldots, y_k$ überführen, sind uns bekannt. Das nicht veröffentlichte k-te Polynom aus (4.4) kann durch das Polynom

$$v'_k = \sum_i u_i u_{i+1}$$

ersetzt werden. Die Koeffizienten des Polynoms hängen nur scheinbar von X und Y ab, denn es gilt:

Lemma 5.23 Im nicht-entarteten Fall nach Forderung 7 sind die Koeffizienten von v'_k unabhängig von X und Y.

Beweis Jeder Koeffizient c der quadratischen Form v'_k hat die Form

$$c = \sum_{0 \le i < k, 0 \le j \le 1} w_{ij} X^i Y^j.$$

Wegen der zyklischen Symmetrie und der Spiegelsymmetrie gibt es $2k$ mögliche Anordnungen für $\delta_1, \ldots, \delta_k$. Für jede der $2k$ Anordnungen der δ_i ergibt sich der gleiche Wert für c. Dies liefert $2k$ lineare Gleichungen in den $2k$ Unbekannten w_{ij}, $0 \le i < k$, $0 \le j \le 1$. Es gibt eine Lösung des Systems mit $w_{00} = c$ und $w_{ij} = 0$ für $(i, j) \neq (0, 0)$. Im nicht-entarteten Fall ist das lineare Gleichungssystem regulär und die Lösung für die $2k$ Unbekannten w_{ij} eindeutig bestimmt. □

Die Koeffizientenvektoren $u_1, \ldots, u_k$, die den linearen Zusammenhang zwischen den ursprünglichen von den neuen Variablen charakterisieren, können in Abhängigkeit von X und Y ausgedrückt werden. Sei A' die Matrix, deren Zeilen aus $u_1, \ldots, u_k$ bestehen. Jeder Eintrag von A' ist ein Element aus der zweifachen Körpererweiterung. Da Polynome dieser Form invertiert werden können, kann mit dem Gauß-Algorithmus die Matrix A' invertiert werden. Es gilt

$$\begin{pmatrix} y_1 \\ \vdots \\ y_k \end{pmatrix} = (A')^{-1} \begin{pmatrix} u_1 \\ \vdots \\ u_k \end{pmatrix}. \tag{5.10}$$

Die Polynome $v_1, \ldots, v_{k-1}$ des öffentlichen Schlüssels sowie v'_k sind quadratische Formen in den Variablen $y_1, \ldots, y_k$. Mit (5.10) erhält man $v_1, \ldots, v_{k-1}, v'_k$ als quadratische Form in den Variablen $u_1, \ldots, u_k$ (im folgenden setzen wir $v_k := v'_k$):

$$v_i = \sum_j b'_{ij} u_j u_{j+1}, 1 \leq i \leq k.$$

Durch diese Gleichung wird eine Matrix B' definiert.

Die Einträge der Matrizen A' und B' sind Elemente aus der zweifachen Körpererweiterung. Das Matrizenpaar (A', B') erzeugt die vorgegebenen Polynome $v_1, \ldots, v_{k-1}$ des öffentlichen Schlüssels. Mit diesen Matrizen kann das Verfahren Unterschreiben einer Nachricht ausgeführt werden. Alle Rechnungen müssen jedoch in der Körpererweiterung durchgeführt werden.

Seien $h_1(m), \ldots, h_{k-1}(m)$ die Stützstellen der Nachricht und $h_k(m)$ beliebig. Gesucht sind Werte für die Produkte $y_i y_j$, so daß

$$\sum_{j,l} (C_i)_{j,l}\, y_j y_l = h_i(m), \quad 1 \leq i \leq k-1,$$

gilt. Die Matrizen $C_1, \ldots, C_{k-1}$ sind die Formenmatrizen der Polynome $v_1, \ldots, v_{k-1}$ des öffentlichen Schlüssels.

Durch Invertieren der Matrix B' in der Körpererweiterung ergeben sich Werte für die Basiselemente $u_1u_2, \ldots, u_ku_1$ in der Körpererweiterung:

$$\begin{pmatrix} u_1u_2 \\ \vdots \\ u_ku_1 \end{pmatrix} = (B')^{-1} \begin{pmatrix} h_1(m) \\ \vdots \\ h_k(m) \end{pmatrix}.$$

Die Inverse der Matrix A' beschreibt die Variablentransformation

$$\begin{pmatrix} y_1 \\ \vdots \\ y_k \end{pmatrix} = (A')^{-1} \begin{pmatrix} u_1 \\ \vdots \\ u_k \end{pmatrix}.$$

Jeder Term vom Grad 2 in den neuen Variablen ist eine Summe von Monomen vom Grad 2 in den ursprünglichen Variablen:

$$y_i y_j = (\sum_{l=1}^{k} (a'^{-1})_{il} \cdot u_l)(\sum_{l=1}^{k} (a'^{-1})_{jl} \cdot u_l), \quad 1 \leq i, j \leq k.$$

Die Werte für die Produkte $y_i y_j$ stammen zwar formal aus der Körpererweiterung, sind jedoch im nicht-entarteten Fall gemäß Forderung 7 unabhängig von X und Y. Das Argument ist das gleiche Symmetrieargument, das schon bei der Lemma 5.23 verwendet wurde:

Da die Werte für die Produkte $y_i y_j$ unabhängig von den $2k$ möglichen δ-Anordnungen sind, sind sie unabhängig von (X, Y).

Wir haben damit Werte für die Produkte $y_i y_{i+1}$, $1 \leq i \leq k$, in Abhängigkeit vom öffentlichen Schlüssel, den Stützstellen $h_1(m), \ldots, h_{k-1}(m)$ und dem beliebigen Wert für $h_k(m)$ ermittelt. Da die gefundenen Werte die $k-1$ Kongruenzen

$$\sum_{j,l} (C_i)_{j,l}\, y_j y_l = h_i(m), \quad 1 \leq i \leq k-1,$$

erfüllen, haben wir eine gültige Unterschrift gefunden.

5.4 Zusammengesetzte Moduln

Wenn n eine Primzahl ist, hat das Polynom $P(\delta)$ k Nullstellen modulo n. Ist n ein zusammengesetzter Modul der Form $p \cdot q$, dann hat das Polynom $P(\delta)$ jedoch k^2 Nullstellen modulo n. Jede Lösung modulo p kann mit jeder Lösung modulo q kombiniert werden. Es gibt folglich eine zyklische Anordnung der k Werte für δ modulo p und eine davon unabhängige zyklische Anordnung der k Werte für δ modulo q. Unsere Berechnungen können jedoch trotzdem modulo n durchgeführt werden, weil wir stets nur die Polynome und symbolische Fixierungen, aber an keiner Stelle die expliziten Werte der Nullstellen verwenden. Die Polynome modulo p und die Polynome modulo q können mit Hilfe des Chinesischen Restsatzes zusammengesetzt werden, um die Rechnungen auf den Modul n zu übertragen.

5.5 Sonderfälle

In diesem Abschnitt sollen die Bedingungen 5.7 für den nicht-entarteten Fall beurteilt werden.

Zu Forderung 1 (sie wird bei der Herleitung von Lemma 5.10 verwendet). Für zufällige Teilräume U_i und T ist die Voraussetzung mit großer Wahrscheinlichkeit erfüllt. Bei zufälliger Wahl der Transformationen ist die Voraussetzung auch für die Teilräume des Angriffs mit großer Wahrscheinlichkeit erfüllt.

Zu Forderung 2 (sie wird bei dem Verfahren zur Elimination der Koeffizienten $\epsilon_3, \ldots, \epsilon_{k-1}$ verwendet). Vom Standpunkt der algebraischen Bedingungen charakterisieren die Polynomgleichungen die gesuchten Tupel $(\delta_i, \epsilon_{3,i}, \ldots, \epsilon_{k-1,i})$, $1 \leq i \leq k$, eindeutig. Wegen der Vielzahl der Gleichungen vermuten wir, daß die beschriebene Auflösung in den meisten Fällen zum Erfolg führt.

Zu Forderung 3 (sie wird im Beweis von Lemma 5.17 verwendet). Bei zufälliger Wahl der Transformationsmatrizen sind α_i, β_i mit großer Wahrscheinlichkeit ungleich Null, $1 \leq i \leq k$.

Zu Forderung 4 (sie wird bei der Normierung der mit Lemma 5.17 gewonnenen Koeffizientenvektoren $u_1, \ldots, u_k$ verwendet). Bei zufälliger Wahl der Transformationsmatrizen ist die Forderung mit großer Wahrscheinlichkeit erfüllt.

Zu Forderung 5 (sie wird bei der Konstruktion der quadratischen Gleichung verwendet). Vom Standpunkt der algebraischen Bedingungen können δ_2 und δ_5 bei festem δ_1 von δ_3 und δ_4 unterschieden werden. Das Verfahren benutzt die Gleichungen, mit denen die Unterscheidung durchgeführt werden kann, und bringt sie auf die Form einer quadratischen Gleichung. Weil die Unterscheidung vom Standpunkt der algebraischen Bedingungen möglich ist, vermuten wir, daß die Transformation auf die Form der quadratischen Gleichung in den meisten Fällen zum Erfolg führt.

Zu Forderung 6 (sie wird bei der Konstruktion von $(K[X]/P(X))[Y]/Q(X,Y)$ benutzt). Wir benötigen, daß die Elemente von $(K[X]/P(X))[Y]/Q(X,Y)$ invertierbar sind. Die meisten Elemente der Menge erfüllen diese Eigenschaft.

Zu Forderung 7 (sie wird benötigt, um in Lemma 5.23 und beim Unterzeichnen einer Nachricht die Unabhängigkeit von den fixierten Werten zu zeigen). Wir können nicht beweisen, daß die konstruierten Gleichungssysteme mit $2k$ Gleichungen in $2k$ Unbekannten regulär sind. Unsere Vermutung, daß die Forderung mit großer Wahrscheinlichkeit erfüllt ist, wird durch Experimente bestätigt. In Hinblick auf allgemeine Zusammenhänge bezüglich Symmetrien in polynomialen Gleichungssystemen bleiben an dieser Stelle jedoch offene Fragen.

5.6 Der Fall $k \neq 5$

Bei der symmetrischen Basis ist die Zahl k der Variablen eine ungerade Zahl größer oder gleich 3 (siehe Lemma 4.5). Für den Fall $k = 3$ geben Coppersmith, Stern und Vaudenay (1993) einen speziellen Angriff an, der das Problem direkt auf den Pollard-Algorithmus aus Abschnitt 3.1.2 reduziert.

Das zentrale Lemma 5.10, das auf die algebraischen Bedingungen für $\delta_1, \ldots, \delta_k$ führt, gilt für alle ungeraden $k \geq 5$. Ebenso lassen sich die für den Angriff zentralen Symmetrieüberlegungen auf alle ungeraden $k \geq 5$ übertragen.

Bei der Umsetzung der algebraischen Bedingungen muß im Fall $k > 5$ analysiert werden, mit Hilfe welcher Gleichungen die Unterscheidungen zwischen den Räumen durchgeführt werden können. Praktische Probleme beim Angriff auf die symmetrische Basis mit $k \geq 7$ bereiten die großen Polynome, die vor der Konstruktion der quadratischen Gleichung entstehen. Ein Polynom, das mit dem beschriebenen Verfahren reduziert wird, kann aus bis zu $k!$ Termen bestehen. Im Fall $k = 7$ sind dies $7! = 5040$ Terme.

5.7 Beispiel

Sei $k = 5$, $n = p \cdot q = 7853 \cdot 8647 = 67904891$. Um extrem große Zahlen zu vermeiden, werden alle Zahlen modulo p angegeben.

Die geheimen Transformationen:

$$A = \begin{pmatrix} 936 & 75 & 494 & 559 & 229 \\ 70 & 868 & 624 & 42 & 975 \\ 855 & 568 & 573 & 532 & 227 \\ 670 & 96 & 705 & 225 & 5 \\ 724 & 437 & 247 & 928 & 818 \end{pmatrix}, \quad B = \begin{pmatrix} 684 & 53 & 821 & 512 & 509 \\ 951 & 651 & 172 & 252 & 776 \\ 468 & 610 & 618 & 892 & 293 \\ 476 & 300 & 750 & 899 & 126 \\ 365 & 404 & 502 & 863 & 190 \end{pmatrix}.$$

Die Matrizen des öffentlichen Schlüssels lauten

$$C_1 = \begin{pmatrix} 5219 & 1117 & 5422 & 5853 & 6862 \\ 1117 & 6938 & 3613 & 4119 & 4147 \\ 5422 & 3613 & 2186 & 5111 & 2601 \\ 5853 & 4119 & 5111 & 5314 & 7015 \\ 6862 & 4147 & 2601 & 7015 & 6787 \end{pmatrix}, \quad C_2 = \begin{pmatrix} 5378 & 3473 & 3294 & 6529 & 3641 \\ 3473 & 5195 & 320 & 4412 & 5757 \\ 3294 & 320 & 2837 & 4647 & 1943 \\ 6529 & 4412 & 4647 & 2940 & 791 \\ 3641 & 5757 & 1943 & 791 & 4516 \end{pmatrix},$$

$$C_3 = \begin{pmatrix} 4571 & 6786 & 5226 & 716 & 6281 \\ 6786 & 4888 & 2792 & 3697 & 3276 \\ 5226 & 2792 & 5694 & 1574 & 7158 \\ 716 & 3697 & 1574 & 5102 & 3674 \\ 6281 & 3276 & 7158 & 3674 & 33 \end{pmatrix}, \quad C_4 = \begin{pmatrix} 288 & 4854 & 2161 & 2573 & 3586 \\ 4854 & 4750 & 3198 & 2663 & 5886 \\ 2161 & 3198 & 6791 & 5145 & 6650 \\ 2573 & 2663 & 5145 & 125 & 7462 \\ 3586 & 5886 & 6650 & 7462 & 5922 \end{pmatrix}.$$

Die erste der 55 Minorengleichungen:

$$\begin{aligned} & 7286 + 3262\delta + 6776\delta^2 + 758\delta^3 + 1603\epsilon_3 + 4881\delta\epsilon_3 \\ + \; & 2071\delta^2\epsilon_3 + 3488\epsilon_3^2 + 2362\delta\epsilon_3^2 + 1902\epsilon_3^3 + 6618\epsilon_4 + 7747\delta\epsilon_4 \\ + \; & 6533\delta^2\epsilon_4 + 954\epsilon_3\epsilon_4 + 2443\delta\epsilon_3\epsilon_4 + 6815\epsilon_3^2\epsilon_4 + 3090\epsilon_4^2 + 789\delta\epsilon_4^2 \\ + \; & 1173\epsilon_3\epsilon_4^2 + 6749\epsilon_4^3 = 0 \end{aligned}$$

Gleichung für ϵ_3 in Abhängigkeit von ϵ_4, δ:

$$\epsilon_3(\delta, \epsilon_4) = 2914 + 4299\delta + 6098\delta^2 + 6782\delta^3 + 3721\epsilon_4$$

Gleichung für ϵ_4 in Abhängigkeit von δ:

$$\epsilon_4(\delta) = 6627 + 2112\delta + 4093\delta^2 + 5791\delta^3 + 1587\delta^4$$

Die Polynomgleichung in δ vom Grad 5:

$$6319 + 5998\delta + 2563\delta^2 + 4338\delta^3 + 5244\delta^4 + \delta^5 = 0$$

Die Verschiedenheit der Nullstellen liefert Polynome kleineren Grades:

$$P_2(\delta_2) = 5998 + 2563\delta_1 + 4338\delta_1^2 + 5244\delta_1^3 + \delta_1^4 + 2563\delta_2 + 4338\delta_1\delta_2 + 5244\delta_1^2\delta_2$$

$$
\begin{aligned}
& & & +\delta_1^3\delta_2 + 4338\delta_2^2 + 5244\delta_1\delta_2^2 + \delta_1^2\delta_2^2 + 5244\delta_2^3 + \delta_1\delta_2^3 + \delta_2^4 \\
P_3(\delta_3) &= & & 2563 + 4338\delta_1 + 5244\delta_1^2 + \delta_1^3 + 4338\delta_2 + 5244\delta_1\delta_2 + \delta_1^2\delta_2 + 5244\delta_2^2 \\
& & & +\delta_1\delta_2^2 + \delta_2^3 + 4338\delta_3 + 5244\delta_1\delta_3 + \delta_1^2\delta_3 + 5244\delta_2\delta_3 + \delta_1\delta_2\delta_3 + \delta_2^2\delta_3 \\
& & & +5244\delta_3^2 + \delta_1\delta_3^2 + \delta_2\delta_3^2 + \delta_3^3 \\
P_4(\delta_4) &= & & 4338 + 5244\delta_1 + \delta_1^2 + 5244\delta_2 + \delta_1\delta_2 + \delta_2^2 + 5244\delta_3 + \delta_1\delta_3 \\
& & & +\delta_2\delta_3 + \delta_3^2 + 5244\delta_4 + \delta_1\delta_4 + \delta_2\delta_4 + \delta_3\delta_4 + \delta_4^2 \\
P_5(\delta_5) &= & & 5244 + \delta_1 + \delta_2 + \delta_3 + \delta_4 + \delta_5
\end{aligned}
$$

Die quadratische Gleichung in Y:

$$
\begin{aligned}
& 1844 + 5446X + 4441X^2 + 1778X^3 + 6277X^4 \\
+\ & 3151Y + 2052XY + 3035X^2Y + 1474X^3Y + 5732X^4Y \\
+\ & 6773Y^2 + 6440XY^2 + 1969X^2Y^2 + 3133X^3Y^2 + 3332X^4Y^2 \\
=\ & 0
\end{aligned}
$$

Die Gleichung mit linearem Auftreten von δ_3:

$$
\begin{aligned}
& 3151 + 6773X + 2052Y + 6440XY + 3035Y^2 \\
+\ & 1969XY^2 + 1474Y^3 + 3133XY^3 + 5732Y^4 + 3332XY^4 \\
+\ & (6773 + 6440Y + 1969Y^2 + 3133Y^3 + 3332Y^4)\ \delta_3 = 0
\end{aligned}
$$

Das Auflösen nach δ_3 erfordert eine Invertierung in der zweifachen Körpererweiterung. Es ergibt sich

$$
\begin{aligned}
\delta_3 &= 1473 + 1480X + 4713X^2 + 3966X^3 + 5175X^4 \\
& \quad +4438Y + 7645XY + 7626X^2Y + 4637X^3Y + 5607X^4Y.
\end{aligned}
$$

Analog erhält man

$$
\begin{aligned}
\delta_4 &= 710 + 5276X + 1673X^2 + 2176X^3 + 3161X^4 \\
& \quad +3415Y + 208XY + 227X^2Y + 3216X^3Y + 2246X^4Y, \\
\delta_5 &= 426 + 1096X + 1467X^2 + 1711X^3 + 7370X^4 + 7852Y.
\end{aligned}
$$

Die Formenmatrix C_5' des neu konstruierten Polynoms v_5' lautet

$$
C_5' = \begin{pmatrix}
5 & 1796 & 4031 & 4274 & 3570 \\
1796 & 7658 & 6274 & 103 & 1990 \\
4031 & 6274 & 1148 & 2335 & 7834 \\
4274 & 103 & 2335 & 1846 & 4067 \\
3570 & 1990 & 7834 & 4067 & 90
\end{pmatrix}.
$$

Die ermittelte Unterschrift ist

$$
(y_1y_2, \ldots, y_5y_1)^T = (25, 2962, 4752, 6631, 5867)^T.
$$

Kapitel 6

Der Angriff auf die asymmetrische Basis

In diesem Kapitel wird gezeigt, wie das Signaturschema bei Wahl der asymmetrischen Basis $\{u_1^2, u_1u_2, \ldots, u_{k-1}u_k\}$ gebrochen werden kann. Wir betrachten zunächst $k = 5$ und dann $k = 4$. In Hinblick auf die vermeintliche Sicherheit und den benötigten Rechenaufwand des Kryptosystems sind dies die interessantesten Fälle. Für einen gegebenen öffentlichen Schlüssel kann der geheime Schlüssel ermittelt werden.

6.1 Rekonstruktion des geheimen Schlüssels

Die Berechnungen werden zunächst unter der Voraussetzung ausgeführt, daß der Modul n eine Primzahl ist. Für den Angriff seien die folgenden Bedingungen erfüllt.

Nicht-Entartungsbedingungen 6.1

1. Im Verlauf des Angriffs werden ein k-dimensionaler Vektorraum V sowie Teilräume U_i und T konstruiert. U_i ist ein zweidimensionaler Unterraum von V und T ein $(k-2)$-dimensionaler affiner Teilraum von V.
   Forderung: $U_i \cap T$ sei von der Dimension Null.

2. Im Verlauf des Angriffs wird ein Gleichungssystem in den Variablen $\delta, \epsilon_3, \ldots, \epsilon_{k-1}$ konstruiert. Es wird ein Verfahren angegeben, mit dem $\epsilon_3, \ldots, \epsilon_{k-1}$ in Abhängigkeit von δ ausgedrückt werden können und mit dem ein Polynom vom Grad k in δ berechnet werden kann.
   Forderung: Das Verfahren führe zum Erfolg.

3. Im Verlauf des Angriffs werden Körperelemente α_i und β_i verwendet, von denen nicht bekannt sind, ob sie ungleich Null sind.
   Forderung: α_i und β_i seien ungleich Null.

4. Sei A die Variablentransformation des geheimen Schlüssels.
   Forderung: In der ersten Spalte von A seien alle Einträge von Null verschieden.

6.1.1 Struktur der Formenmatrizen

Lemma 6.2 Sei $k \geq 4$. Eine Linearkombination der Basiselemente $u_1^2, u_1u_2, \ldots, u_{k-1}u_k$. ist genau dann eine quadratische Form vom Rang kleiner oder gleich 2 sind, wenn sie eine der Formen

$$\begin{array}{rrcll} & \alpha_1 u_1 u_2 & + & \beta_1 u_2 u_3 & (\text{Typ } 1), \\ & \alpha_2 u_2 u_3 & + & \beta_2 u_3 u_4 & (\text{Typ } 2), \\ & & \vdots & & \\ & \alpha_{k-2} u_{k-2} u_{k-1} & + & \beta_{k-2} u_{k-1} u_k & (\text{Typ } k-2) \\ \text{oder} & \alpha_{k-1} u_1^2 & + & \beta_{k-1} u_1 u_2 & (\text{Typ } k-1) \end{array} \tag{6.1}$$

mit $\alpha_i, \beta_i \in \mathbb{Z}_n$, $1 \leq i \leq k-1$, hat.

Beweis Sei

$$a_1 u_1^2 + \sum_{i=2}^{k} a_i \, u_{i-1} u_i, \quad a_1, \ldots, a_k \in \mathbb{Z}_n \tag{6.2}$$

eine Linearkombination der Basiselemente und Q die zugeordnete Formenmatrix.

Die Matrix Q lautet (zur besseren Übersicht werden nur die Einträge aufgeführt, die von Null verschieden sein können)

$$Q = \frac{1}{2} \begin{pmatrix} 2a_1 & a_2 & & & & \\ a_2 & & a_3 & & & \\ & a_3 & & a_4 & & \\ & & a_4 & & \ddots & \\ & & & \ddots & & a_k \\ & & & & a_k & \end{pmatrix}.$$

"$\Longleftarrow$" Für eine Linearkombination (6.2) vom Typ $t \in \{1, \ldots, k-1\}$ folgt unmittelbar, daß die Formenmatrix Q einen Rang kleiner oder gleich 2 hat.

"$\Longrightarrow$" **Annahme:** Die Linearkombination (6.2) sei nicht von der Form (6.1).

Fall 1: $a_1 = 0$.

Die Matrix Q lautet

$$Q = \frac{1}{2} \begin{pmatrix} 0 & a_2 & & & & \\ a_2 & & a_3 & & & \\ & a_3 & & a_4 & & \\ & & a_4 & & \ddots & \\ & & & \ddots & & a_k \\ & & & & a_k & \end{pmatrix}.$$

Für $j := \min\{i \in \{2,\ldots,k\} : a_i \neq 0\}$, $l := \max\{i \in \{2,\ldots,k\} : a_i \neq 0\}$ gilt $l - j \geq 2$. Die Untermatrix

$$\frac{1}{2}\begin{pmatrix} 0 & a_j & 0 \\ a_j & 0 & x \\ 0 & 0 & a_l \end{pmatrix} \quad \text{mit } x := \begin{cases} 0, & \text{wenn } l-j>2 \\ a_{j+1}, & \text{wenn } l-j=2 \end{cases}$$

von Q hat Determinante $-(\frac{1}{2})^3 a_j^2 a_l \neq 0$. Mit Fakt 5.2 folgt $\text{Rang}(Q) \geq 3$.

Fall 2: $a_1 \neq 0$

Sei $j := \min\{i \in \{3,\ldots,k\} : a_i \neq 0\}$. Die linke obere $j \times j$-Untermatrix von Q lautet

$$\frac{1}{2}\begin{pmatrix} 2a_1 & a_2 & & & & & \\ a_2 & & 0 & & & & \\ & 0 & & \ddots & & & \\ & & \ddots & & 0 & & \\ & & & 0 & & a_j & \\ & & & & a_j & & \end{pmatrix}.$$

Die Untermatrix

$$\frac{1}{2}\begin{pmatrix} 2a_1 & x & 0 \\ x & 0 & a_j \\ 0 & a_j & 0 \end{pmatrix} \quad \text{mit } x := \begin{cases} 0, & \text{wenn } j>3 \\ a_2, & \text{wenn } j=3 \end{cases}$$

hat Determinante $-(\frac{1}{2})^2 a_1 a_j^2 \neq 0$. Mit Fakt 5.2 folgt $\text{Rang}(Q) \geq 3$. □

Von nun an wird nur noch der Fall $k = 5$ betrachtet.

Bemerkung 6.3 Im Fall $k = 5$ lauten die in (6.1) eingeführten Typen quadratischer Formen

$$\begin{array}{ll} \alpha_1 u_1 u_2 + \beta_1 u_2 u_3 & \text{(Typ 1)}, \\ \alpha_2 u_2 u_3 + \beta_2 u_3 u_4 & \text{(Typ 2)}, \\ \alpha_3 u_3 u_4 + \beta_3 u_4 u_5 & \text{(Typ 3)}, \\ \alpha_4 u_1^2 + \beta_4 u_1 u_2 & \text{(Typ 4)} \end{array} \tag{6.3}$$

mit $\alpha_i, \beta_i \in \mathbb{Z}_n$, $1 \leq i \leq 4$.

Lemma 6.4 Für $k = 5$ seien $v_1, \ldots, v_{k-1}$ die durch (4.2) definierten Polynome des öffentlichen Schlüssels. Dann gilt: Für jedes $i \in \{1,\ldots,4\}$ gibt es genau ein Paar $(\alpha_i, \beta_i) \in \mathbb{Z}_n^2$ und genau ein Tripel $(\delta, \epsilon_3, \epsilon_4) \in \mathbb{Z}_n^3$, so daß die quadratische Form des Typs i aus (6.3) mittels

$$v_1 + \delta v_2 + \epsilon_3 v_3 + \epsilon_4 v_4$$

dargestellt werden kann, d.h.

$$\begin{array}{llll}
\exists_1(\alpha_1,\beta_1) & \exists_1(\delta_1,\epsilon_{3,1},\epsilon_{4,1}) & \alpha_1 u_1 u_2 + \beta_1 u_2 u_3 = v_1 + \delta_1 v_2 + \epsilon_{3,1} v_3 + \epsilon_{4,1} v_4, \\
\exists_1(\alpha_2,\beta_2) & \exists_1(\delta_2,\epsilon_{3,2},\epsilon_{4,2}) & \alpha_2 u_2 u_3 + \beta_2 u_3 u_4 = v_1 + \delta_2 v_2 + \epsilon_{3,2} v_3 + \epsilon_{4,2} v_4, \\
\exists_1(\alpha_3,\beta_3) & \exists_1(\delta_3,\epsilon_{3,3},\epsilon_{4,3}) & \alpha_3 u_3 u_4 + \beta_3 u_4 u_5 = v_1 + \delta_3 v_2 + \epsilon_{3,3} v_3 + \epsilon_{4,3} v_4, \\
\exists_1(\alpha_4,\beta_4) & \exists_1(\delta_4,\epsilon_{3,4},\epsilon_{4,4}) & \alpha_4 u_1^2 + \beta_4 u_1 u_2 = v_1 + \delta_4 v_2 + \epsilon_{3,4} v_3 + \epsilon_{4,4} v_4.
\end{array}$$

Beweis Betrachte den linearen Raum V der Linearkombinationen $a_1\, u_1^2 + \sum_{i=2}^{5} a_i\, u_{i-1} u_i$ für beliebige $a_i \in \mathbb{Z}_n$, $1 \le i \le 5$. Der Vektorraum V hat Dimension 5.

Die Linearkombinationen des Typs i für beliebige $\alpha_i, \beta_i \in \mathbb{Z}_n$ bilden einen zweidimensionalen Unterraum U_i von V.

Die Formen $v_1+\delta v_2+\epsilon_3 v_3+\epsilon_4 v_4$ mit beliebigen Koeffizienten $\delta, \epsilon_3, \epsilon_4 \in \mathbb{Z}_n$ bilden einen Unterraum T der Dimension kleiner oder gleich 3 von V. Die quadratischen Formen $v_1, \ldots, v_4$ sind linear unabhängig, weil die Matrix B aus (4.2) regulär ist. Damit gilt $\dim T = 3$. Im nicht-entarteten Fall gemäß Forderung 1 ist $U_i \cap T$ von der Dimension Null. □

Das Lemma 6.4 hat eine zentrale Bedeutung. Die Bezeichnungen α_i, β_i, δ_i, $\epsilon_{3,i}$, $\epsilon_{4,i}$, $1 \le i \le 4$, sollen im folgenden wie in Lemma 6.4 definiert sein.

6.1.2 Elimination der Koeffizienten

Nach Lemma 6.2 und Lemma 6.4 gibt es genau 4 verschiedene Tripel $(\delta_i, \epsilon_{3,i}, \epsilon_{4,i})$, $1 \le i \le 4$, für die die quadratische Form

$$v_1 + \delta_i v_2 + \epsilon_{3,i} v_3 + \epsilon_{4,i} v_4$$

vom Rang kleiner oder gleich 2 ist, $1 \le i \le 4$.

Im nicht-entarteten Fall im Sinne von Forderung 2 können wie bei der symmetrischen Basis in Abschnitt 5.3.2 Polynome $\epsilon_3(\delta), \epsilon_4(\delta), P(\delta) \in \mathbb{Z}_n[\delta]$ berechnet werden, so daß gilt:

- $\delta_1, \ldots, \delta_4$ sind Nullstellen von $P(\delta)$. $P(\delta)$ hat keine weiteren Nullstellen.
- $(\delta_i, \epsilon_3(\delta_i), \epsilon_4(\delta_i)) = (\delta_i, \epsilon_{3,i}, \epsilon_{4,i}), \quad 1 \le i \le 4.$

Es gilt

Lemma 6.5 δ_4 ist eine mindestens zweifache Nullstelle von $P(\delta)$.

Beweis Sei $F(\delta)$ die Formenmatrix von $v_1+\delta v_2+\epsilon_3(\delta)v_3+\epsilon_4(\delta)v_4$ in den ursprünglichen Variablen. Nach (6.3) gilt

$$F(\delta_4) = \frac{1}{2}\begin{pmatrix} 2\alpha_4 & \beta_4 & 0 & 0 & 0 \\ \beta_4 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Jede Untermatrix der Ordnung 3 von $F(\delta_4)$ hat mindestens eine Nullspalte und eine Nullzeile. Wie bei Gleichung (3.4) im Angriff auf das Schema der sequentiellen Linearisierung folgt: δ_4 ist eine mindestens zweifache Nullstelle jedes Minors dritter Ordnung von $F(\delta)$.

$P(\delta)$ entsteht durch Linearkombinationen der Minoren dritter Ordnung in den neuen Variablen. Mit Lemma 3.2 folgt die Behauptung. □

Bemerkung 6.6 Im nicht-entarteten Fall gemäß Forderung 2 gilt:

- $\delta_1, \ldots, \delta_4$ sind paarweise verschieden.
- $\delta_1, \ldots, \delta_3$ sind einfache Nullstellen von $P(\delta)$, δ_4 ist eine doppelte Nullstelle von $P(\delta)$.
- Das Polynom $P(\delta)$ hat *genau* den Grad $k = 5$.

6.1.3 Charakterisierung der Variablentransformation

Wir verwenden die gleichen Bezeichnungen wie beim Angriff auf die symmetrische Basis: τ sei die Formenmatrix von

$$v_1 + \delta v_2 + \epsilon_3 v_3 + \epsilon_4 v_4.$$

τ ist nach der Ersetzung der Koeffizienten ϵ_3 und ϵ_4 durch die polynomialen Ausdrücke in δ eine Matrix in Abhängigkeit von δ.

Y_i bezeichne den Spaltenraum von $\tau(\delta)$ an der Stelle $\delta = \delta_i$, $1 \leq i \leq 4$. u_i bezeichne zusätzlich den Koeffizientenvektor, welcher die Transformation der Variable u_i in die Variablen $y_1, \ldots, y_k$ beschreibt, $1 \leq i \leq k$.

Lemma 6.7 Es gilt

$$\begin{aligned} Y_1 &= \operatorname{span}(u_2, \alpha_1 u_1 + \beta_1 u_3), \\ Y_2 &= \operatorname{span}(u_3, \alpha_2 u_2 + \beta_2 u_4), \\ Y_3 &= \operatorname{span}(u_4, \alpha_3 u_3 + \beta_3 u_5), \\ Y_4 &= \operatorname{span}(u_1, \alpha_4 u_1 + \beta_4 u_2). \end{aligned}$$

Beweis Y_1 ist der Spaltenraum der Formenmatrix von

$$\alpha_1 u_1 u_2 + \beta_1 u_2 u_3 = u_2 \cdot (\alpha_1 u_1 + \beta_1 u_3)$$

in den neuen Variablen. Die Aussage für Y_1 folgt aus Satz 5.3. Für Y_2, Y_3 und Y_4 folgen die Aussagen in gleicher Weise. □

Die Koeffizientenvektoren $u_1, \ldots, u_5$ lassen sich mit Hilfe der Zeilenräume $Y_1, \ldots, Y_5$ charakterisieren.

Lemma 6.8 Es gilt

$$\begin{array}{lcll} u_1 & \in & Y_4 \cap (Y_1 + Y_2) & \text{(Dimension 2)}, \\ u_2 & \in & Y_1 \cap (Y_2 + Y_3) \cap Y_4 & \text{(Dimension 1)}, \\ u_3 & \in & Y_2 \cap (Y_1 + Y_4) & \text{(Dimension 1)}, \\ u_4 & \in & Y_3 \cap (Y_2 + Y_1) \cap (Y_2 + Y_4) & \text{(Dimension 1)}, \\ u_5 & \in & Y_2 + Y_3 & \text{(Dimension 4)}. \end{array}$$

Beweis Nach der dritten Nicht-Entartungsbedingung gilt $\alpha_i, \beta_i \neq 0$. Die Aussagen lassen sich analog zu Lemma 5.17 bei der symmetrischen Basis nachrechnen. Die von 1 verschiedenen Dimensionen folgen aus

$$\begin{array}{rcl} Y_4 \cap (Y_1 + Y_2) & = & \mathrm{span}(u_1, \alpha_4 u_1 + \beta_4 u_2) \cap \mathrm{span}(u_2, \alpha_1 u_1 + \beta_1 u_3, u_3, \alpha_2 u_2 + \beta_2 u_4) \\ & = & \mathrm{span}(u_1, u_2) \cap \mathrm{span}(u_1, u_2, u_3, u_4) \\ & = & \mathrm{span}(u_1, u_2), \\ Y_2 + Y_3 & = & \mathrm{span}(u_3, \alpha_2 u_2 + \beta_2 u_4, u_4, \alpha_3 u_3 + \beta_3 u_5) \\ & = & \mathrm{span}(u_2, u_3, u_4, u_5). \end{array}$$

□

Im Gegensatz zur symmetrischen Basis können die Werte für $\delta_1, \ldots, \delta_4$ und $u_1, \ldots, u_5$ unterschieden und explizit ermittelt werden.

6.1.4 Reduktion der Polynome

Sei $Q(\delta)$ das Polynom, dessen Nullstellen δ_1, δ_2 und δ_3 sind. $Q(\delta)$ hat den Grad 3. Jedes Vorkommen einer Variablen δ_i kann auf den Grad 2 reduziert werden, indem Vielfache von $Q(\delta_i)$ subtrahiert werden, $1 \leq i \leq 3$. Um zu gewährleisten, daß δ_1, δ_2 und δ_3 verschiedene Nullstellen sind, definieren wir

$$\begin{array}{rcl} Q_2(\delta) & = & \dfrac{Q(\delta) - Q(\delta_1)}{\delta - \delta_1}, \\ Q_3(\delta) & = & \dfrac{Q_2(\delta) - Q_2(\delta_2)}{\delta - \delta_2} \end{array}$$

Es gilt

$$Q_2(\delta_2) = 0, \quad Q_2(\delta_3) = 0, \quad Q_3(\delta_3) = 0.$$

$Q_2(\delta_2)$ ist vom Grad 2 in δ_2, $Q_3(\delta_3)$ ist vom Grad 1 in δ_3. Deshalb kann jedes Auftreten von δ_2 auf den Grad 1 reduziert werden. Jedes Vorkommen von δ_3 kann eliminiert werden.

6.1.5 Sukzessive Berechnung der Variablentransformation

Die Koeffizientenvektoren $u_1, \ldots, u_4$ sind eindeutig bestimmt bis auf multiplikative Konstanten. Die erste Komponente von $u_1, \ldots, u_4$ kann im nicht-entarteten Fall (siehe Forderung 4) durch Anwendung von Lemma 4.7 auf 1 normiert werden. u_5 kann nicht eindeutig charakterisiert werden.

Die Techniken, mit denen die algebraischen Bedingungen in polynomiale Gleichungssysteme umgesetzt werden können, sind die gleichen wie in Abschnitt 5.3.3 beim Angriff auf die symmetrische Basis.

Lemma 6.9 u_2 ist der einzige Koeffizientenvektor, der im Schnitt eines Raumes Y_i, $1 \leq i \leq 3$, mit Y_4 liegt, und zwar liegt u_2 in $Y_1 \cap Y_4$. Durch diese Beziehung ist δ_1 eindeutig bestimmt und kann berechnet werden.

Beweis Es gilt $Y_2 \cap Y_4 = \emptyset$, $Y_3 \cap Y_4 = \emptyset$. Der Schnitt $Y_1 \cap (Y_2 + Y_3)$ hat die Dimension 1 und liefert einen polynomialen Ausdruck für u_2. Mit Hilfe der Beziehung $u_2 \in Y_4$ kann eine Polynomgleichung aufgestellt werden. δ_1 ist das einzige Element in $\mathbb{Z}_n$, das sowohl diese Gleichung als auch die Gleichung $Q(\delta) = 0$ erfüllt. Mit Resultanten wird δ_2 eliminiert. Es entsteht eine quadratische Gleichung in δ_1. Der größte gemeinsame Teiler des quadratischen Polynoms und $Q(\delta_1)$ in $\mathbb{Z}_n$ liefert ein lineares Polynom in δ_1. □

Nach der Berechnung von δ_1 kann das Polynom $Q(\delta)$ vom Grad 3 in ein Polynom $R(\delta)$ vom Grad 2 transformiert werden. Sei

$$R_2(\delta) = \frac{R(\delta) - R(\delta_2)}{\delta - \delta_2}$$

Es gilt $R_2(\delta_3) = 0$. $R_2(\delta_3)$ ist vom Grad 1 in δ_3. In beliebigen Polynomgleichungen kann jedes Vorkommen von δ_2 auf den Grad 1 reduziert werden. Jedes Auftreten von δ_3 kann eliminiert werden.

Lemma 6.10 u_3 ist der einzige Koeffizientenvektor, der im Schnitt eines Raumes Y_i, $2 \leq i \leq 3$, mit $(Y_1 + Y_4)$ liegt, und zwar gilt $u_3 \in Y_2 \cap (Y_1 + Y_4)$. Durch diese Beziehung ist δ_2 eindeutig bestimmt und kann berechnet werden.

Beweis Der Schnitt $Y_3 \cap (Y_1 + Y_4)$ ist leer. Deshalb werden δ_2 und δ_3 durch den Schnitt $Y_i \cap (Y_1 + Y_4)$ voneinander ausgezeichnet. Es ergibt sich eine polynomiale Beziehung für u_3 sowie eine Gleichung für δ_2, die von δ_3 nicht erfüllt wird. Die Gleichung kann reduziert werden. Es entsteht eine lineare Gleichung in δ_2. □

Da δ_1, δ_2 und δ_4 bekannt sind, erhalten wir auch den Wert für δ_3. Es ist nicht länger notwendig, in Restklassenringen modulo einem Polynom in δ zu rechnen. Es kann nun mit expliziten Zahlenwerten gerechnet werden.

Lemma 6.11 u_4 ist der einzige Koeffizientenvektor, der im Schnitt $Y_3 \cap (Y_2 + Y_1)$ liegt. Durch diese Beziehung kann u_4 berechnet werden.

Beweis Der Schnitt $Y_3 \cap (Y_2 + Y_1)$ ist eindimensional und liefert eine Gleichung für u_4. □

Lemma 6.12 Aus den Beziehungen $u_1 \in Y_4 \cap (Y_1 + Y_2)$ und der quadratischen Form $u_2 \cdot (\alpha_1 u_1 + \beta_1 u_3)$ kann u_1 berechnet werden.

Beweis Der Schnitt $Y_4 \cap (Y_1 + Y_2)$ hat die Dimension 2. Nicht nur u_1 liegt in diesem Schnitt, sondern auch u_2. Die Formenmatrix der Linearkombination an der Stelle δ_1 korrespondiert zu der quadratischen Form $u_2 \cdot (\alpha_1 u_1 + \beta_1 u_3)$. Wir dividieren die quadratische Form durch die explizit bekannte Linearform u_2 und erhalten die lineare Funktion $\alpha_1 u_1 + \beta_1 u_3$. u_1 kann dadurch von u_2 unterschieden werden, daß u_1 die Bedingung

$$u_1 \in \text{span}(u_3, \alpha_1 u_1 + \beta_1 u_3)$$

erfüllt. Eine Linearkombination $a \cdot u_1 + b \cdot u_2$ mit $b \neq 0$ erfüllt die Bedingung nicht. Dadurch wird u_1 eindeutig charakterisiert und kann berechnet werden. □

Lemma 6.13 Sei u'_5 ein Vektor aus $\text{span}(u_3, u_5)$, so daß u_3 und u'_5 linear unabhängig sind. Dann gilt: Die Menge der Linearkombinationen von $u_1^2, u_1u_2, \ldots, u_4u_5$ und von $u_1^2, u_1u_2, \ldots, u_3u_4, u_4u'_5$ sind identisch. Einen Vektor u'_5 mit der beschriebenen Eigenschaft erhält man aus der quadratischen Form $u_4 \cdot (\alpha_3 u_3 + \beta_3 u_5)$.

Beweis Jede Linearkombination $a_1^2 u_1^2 + \sum_{i=2}^{5} a_i u_{i-1} u_i$ mit $a_1, \ldots, a_5 \in \mathbb{Z}_n$ ist auch eine Linearkombination von $u_1^2, \ldots, u_3u_4, u_4u'_5$, denn

$$a_4 \cdot u_3u_4 + a_5 \cdot u_4u_5 = u_4(a_4 \cdot u_3 + a_5 \cdot u_5) = u_4(a'_4 \cdot u_3 + a'_5 \cdot u'_5) = a'_4 \cdot u_3u_4 + a'_5 \cdot u_4u'_5$$

mit $a'_4, a'_5 \in \mathbb{Z}_n$. Die Aussage gilt analog in der anderen Richtung.

Die Division der bekannten quadratischen Form $u_4 \cdot (\alpha_3 u_3 + \beta_3 u_5)$ durch die Linearform u_4 liefert

$$u'_5 := \alpha_3 u_3 + \beta_3 u_5.$$

□

Die Matrix, die aus den Zeilen $u_1, \ldots, u_4, u'_5$ gebildet wird, kann die Variablentransformation A' ersetzen. Die fehlende fünfte Gleichung kann durch

$$v'_5 = u_1^2 + \sum_{i=1}^{3} u_i u_{i+1} + u_4 u'_5$$

ersetzt werden. Durch Invertieren der Matrix A' können die Polynome $v_1, \ldots, v_4, v'_5$ in den Variablen $u_1, \ldots, u_4, u'_5$ dargestellt werden. Diese Polynome sind Linearkombinationen der Basiselemente. Sie definieren einen Stellvertreter B' für die Matrix B. Das Matrizenpaar (A', B') erzeugt den gleichen öffentlichen Schlüssel wie das Paar (A, B). Der geheime Schlüssel ist gefunden.

6.2 Zusammengesetzte Moduln

An dieser Stelle gibt es einen wesentlichen Unterschied zum Angriff auf die symmetrische Basis. Ist n ein zusammengesetzter Modul der Form $p \cdot q$, dann gibt es k^2 Nullstellen des Polynoms $P(\delta)$ modulo n. Sowohl modulo p als auch modulo q gibt es eine doppelte Nullstelle. Die Reihenfolge $\delta_1, \ldots, \delta_4$ modulo p ist eindeutig, und die Reihenfolge der Nullstellen modulo q ist eindeutig. Obwohl das Polynom $4 \cdot 4 = 16$ verschiedene Nullstellen modulo n hat, gibt es nur eine Folge $\delta_1, \ldots, \delta_4$, die die Eindeutigkeit der Nullstellen modulo p und modulo q erfüllt. Damit lassen sich alle Berechnungen auf den zusammengesetzten Modul n übertragen.

6.3 Sonderfälle

In diesem Abschnitt sollen die Bedingungen 6.1 für den nicht-entarteten Fall beurteilt werden.

Zu Forderung 1 (sie wird bei der Herleitung von Lemma 6.4 verwendet). Für zufällige Teilräume U_i und T ist die Voraussetzung mit großer Wahrscheinlichkeit erfüllt. Bei zufälliger Wahl der Transformationen ist die Voraussetzung auch für die Teilräume des Angriffs mit großer Wahrscheinlichkeit erfüllt.

Zu Forderung 2 (sie wird bei dem Verfahren zur Elimination der Koeffizienten $\epsilon_3, \ldots, \epsilon_{k-1}$ verwendet). Vom Standpunkt der algebraischen Bedingungen charakterisieren die Polynomgleichungen die gesuchten Tupel $(\delta_i, \epsilon_{3,i}, \ldots, \epsilon_{k-1,i})$ eindeutig. Wegen der Vielzahl der Gleichungen vermuten wir, daß die beschriebene Auflösung in den meisten Fällen zum Erfolg führt.

Zu Forderung 3 (sie wird im Beweis von Lemma 6.8 verwendet). Bei zufälliger Wahl der Transformationsmatrizen sind α_i, β_i mit großer Wahrscheinlichkeit ungleich Null, $1 \leq i \leq k$.

Zu Forderung 4 (sie wird bei der Normierung der mit Lemma 6.8 gewonnenen Koeffizientenvektoren $u_1, \ldots, u_{k-1}, u'_k$ verwendet). Bei zufälliger Wahl der Transformationsmatrizen ist die Forderung mit großer Wahrscheinlichkeit erfüllt.

6.4 Der Fall $k = 4$

Im Fall der symmetrischen Basis muß k ungerade sein. Wenn die asymmetrische Basis benutzt wird, ist es möglich, $k = 4$ zu wählen. Auch in diesem Fall kann der geheime Schlüssel rekonstruiert werden. Die meisten Überlegungen des Angriffs mit $k = 5$ lassen sich übertragen. Es muß jedoch gezeigt werden, daß weiterhin alle Werte für die Koeffizienten $\delta_1, \ldots, \delta_{k-1}$ unterschieden werden können.

Im Fall $k = 4$ haben die quadratischen Formen vom Rang kleiner oder gleich 2 die Form

$$\begin{array}{rc} & \alpha_1 u_1 u_2 + \beta_1 u_2 u_3 \quad \text{(Typ 1)}, \\ & \alpha_2 u_2 u_3 + \beta_2 u_3 u_4 \quad \text{(Typ 2)}, \\ \text{oder} & \alpha_3 u_1^2 + \beta_3 u_1 u_2 \quad \text{(Typ 3)}. \end{array}$$

In Hinblick auf die Summe

$$v_1 + \delta v_2 + \epsilon_3 v_3,$$

wird δ_i durch die Form des Typs i definiert, $1 \leq 1 \leq 3$. Dies liefert ein Polynom $P(\delta)$ vom Grad 4. Die doppelte Nullstelle δ_3 kann ermittelt werden, indem der größte gemeinsame Teiler von P und P' ermittelt wird.

Lemma 6.14 Es gilt

$$\begin{aligned} Y_1 &= \text{span}(u_2, \alpha_1 u_1 + \beta_1 u_3), \\ Y_2 &= \text{span}(u_3, \alpha_2 u_2 + \beta_2 u_4), \\ Y_3 &= \text{span}(u_1, \alpha_3 u_1 + \beta_3 u_2). \end{aligned}$$

Lemma 6.15 Die Bedingungen für die Charakterisierung von $u_1, \ldots, u_4$ sind

$$\begin{array}{lcll} u_1 & \in & Y_3 \cap (Y_1 + Y_2) & \text{(Dimension 2)}, \\ u_2 & \in & Y_1 \cap Y_3 & \text{(Dimension 1)}, \\ u_3 & \in & Y_2 \cap (Y_1 + Y_3) & \text{(Dimension 1)}, \\ u_4 & \in & Y_2 + Y_3 & \text{(Dimension 4)}. \end{array}$$

δ_3 und damit Y_3 ist bekannt. u_2 und δ_1 werden durch

$$u_2 \in Y_1 \cap Y_3$$

charakterisiert. Nach der Berechnung von δ_1 ist δ_2 die verbleibende Nullstelle von $P(\delta)$. u_1 und u_3 können analog zum Fall $k = 5$ berechnet werden. u_4 kann durch das Element

$$u_4' = \alpha_2 u_2 + \beta_2 u_4$$

ersetzt werden.

Das weitere Vorgehen erfolgt analog zum Fall $k = 5$.

6.5 Beispiel

Sei $k = 5$ und der Modul $n = p \cdot q = 7853 \cdot 8647$. Die Transformationsmatrizen seien

$$A = \begin{pmatrix} 936 & 75 & 494 & 559 & 229 \\ 70 & 868 & 624 & 42 & 975 \\ 855 & 568 & 573 & 532 & 227 \\ 670 & 96 & 705 & 225 & 5 \\ 724 & 437 & 247 & 928 & 818 \end{pmatrix}, \quad B = \begin{pmatrix} 684 & 53 & 821 & 512 & ,509 \\ 951 & 651 & 172 & 252 & 776 \\ 468 & 610 & 618 & 892 & 293 \\ 476 & 300 & 750 & 899 & 126 \\ 365 & 404 & 502 & 863 & 190 \end{pmatrix}.$$

Um bei der Darstellung des Beispiels extrem große Zahlen zu vermeiden, werden alle weiteren Zahlen modulo p angegeben. Die symmetrischen Matrizen des öffentlichen Schlüssels lauten

$$C_1 = \begin{pmatrix} 2153 & 6906 & 5444 & 4821 & 4167 \\ 6906 & 2217 & 3423 & 2726 & 5159 \\ 5444 & 3423 & 1306 & 839 & 4933 \\ 4821 & 2726 & 839 & 3565 & 959 \\ 4167 & 5159 & 4933 & 959 & 2118 \end{pmatrix}, \quad C_2 = \begin{pmatrix} 6787 & 171 & 3691 & 7801 & 3328 \\ 171 & 4748 & 6402 & 1723 & 7382 \\ 3691 & 6402 & 2652 & 1987 & 4808 \\ 7801 & 1723 & 1987 & 374 & 6905 \\ 3328 & 7382 & 4808 & 6905 & 6785 \end{pmatrix},$$

$$C_3 = \begin{pmatrix} 3087 & 6028 & 7727 & 5383 & 4720 \\ 6028 & 7747 & 4963 & 251 & 5766 \\ 7727 & 4963 & 655 & 7536 & 1080 \\ 5383 & 251 & 7536 & 1957 & 1933 \\ 4720 & 5766 & 1080 & 1933 & 4327 \end{pmatrix}, \quad C_4 = \begin{pmatrix} 3974 & 1655 & 6643 & 1028 & 6987 \\ 1655 & 3987 & 5379 & 4330 & 1815 \\ 6643 & 5379 & 1466 & 3502 & 1609 \\ 1028 & 4330 & 3502 & 5984 & 7264 \\ 6987 & 1815 & 1609 & 7264 & 2898 \end{pmatrix}.$$

Gleichung für ϵ_3 in Abhängigkeit von ϵ_4, δ:

$$\epsilon_3(\delta, \epsilon_4) = 4114 + 5969\delta + 1868\delta^2 + 4890\delta^3 + 2525\epsilon_4$$

Gleichung für ϵ_4 in Abhängigkeit von δ:

$$\epsilon_4(\delta) = 2087 + 1257\delta + 7850\delta^2 + 1152\delta^3 + 755\delta^4$$

Aus dem Polynom in δ vom Grad 5 kann δ_4 bestimmt werden.

$$\begin{aligned} P(\delta) &= 6893 + 865\delta + 3240\delta^2 + 3987\delta^3 + 4768\delta^4 + \delta^5 \\ P'(\delta) &= 865 + 6480\delta + 4108\delta^2 + 3366\delta^3 + 5\delta^4 \\ \gcd(P, P') &= \delta - 4950 \end{aligned}$$

Es folgt $\delta_4 = 4950$.

Das verbleibende Polynom vom Grad 3 ist

$$Q(\delta) = 3719 + 6224\delta + 6815\delta^2 + \delta^3.$$

Die Verschiedenheit der Nullstellen liefert Polynome kleineren Grades:

$$\begin{aligned} Q_2(\delta_2) &= 6224 + 6815\delta_1 + \delta_1^2 + 6815\delta_2 + \delta_1\delta_2 + \delta_2^2, \\ Q_3(\delta_3) &= 6815 + \delta_1 + \delta_2 + \delta_3. \end{aligned}$$

Der Koeffizientenvektor für u_2 kann bestimmt werden.

$$u_2 = \begin{pmatrix} 3545 + 5594\delta_1 + 7211\delta_1^2 \\ 2430 + 3223\delta_1 + 5243\delta_1^2 \\ 5815 + 2763\delta_1 + 4423\delta_1^2 \\ 1580 + 7062\delta_1 + 6221\delta_1^2 \\ 3024 + 5271\delta_1 + 1491\delta_1^2 \end{pmatrix}^T \cdot \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \end{pmatrix}.$$

Der Wert für δ_1 ist 5205.

Das verbleibende Polynom vom Grad 2 mit Lösungen δ_2 und δ_3 ist

$$R(\delta) = 5473 + 4167\delta + \delta^2,$$

ein aus der Verschiedenheit der Nullstellen resultierendes Polynom

$$R_2(\delta) = 4167 + \delta_2 + \delta_3.$$

Die Beziehung für u_3 lautet

$$u_3 = \begin{pmatrix} 2432 + 5267\delta_2 \\ 4465 + 4422\delta_2 \\ 4285 + 3138\delta_2 \\ 411 + 1450\delta_2 \\ 4048 + 2253\delta_2 \end{pmatrix}^T \cdot \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \end{pmatrix}.$$

Es ergibt sich $\delta_2 = 1595$, $\delta_3 = 2091$ und

$$\begin{aligned} u_4 &= (2959, 213, 828, 7616, 4183) \cdot (y_1, \ldots, y_5)^T, \\ u_1 &= (3915, 6581, 103, 5283, 6168) \cdot (y_1, \ldots, y_5)^T, \\ u_5' &= (623, 1900, 1900, 747, 659) \cdot (y_1, \ldots, y_5)^T. \end{aligned}$$

Die Variablentransformation A':

$$A' = \begin{pmatrix} 3915 & 6581 & 103 & 5283 & 6168 \\ 4890 & 5665 & 3204 & 2934 & 3043 \\ 587 & 5561 & 7034 & 4379 & 909 \\ 2959 & 213 & 828 & 7616 & 4183 \\ 623 & 1900 & 1900 & 747 & 659 \end{pmatrix}.$$

Die Formenmatrix der fehlenden fünften Gleichung:

$$C_5' = \begin{pmatrix} 412 & 4790 & 6093 & 3711 & 2245 \\ 4790 & 3156 & 3975 & 7208 & 2991 \\ 6093 & 3975 & 1594 & 7813 & 7386 \\ 3711 & 7208 & 7813 & 1858 & 152 \\ 2245 & 2991 & 7386 & 152 & 513 \end{pmatrix}.$$

Die Matrix B', die die Linearkombinationen beschreibt:

$$B' = \begin{pmatrix} 1002 & 2720 & 5454 & 4063 & 1482 \\ 4493 & 3035 & 2520 & 3937 & 408 \\ 6472 & 190 & 6315 & 445 & 6145 \\ 5106 & 4728 & 3318 & 777 & 552 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Die Matrizen A' und B' bilden den geheimen Schlüssel.

Kapitel 7

Der Angriff auf die zentrierte Basis

Es wird nun das Signaturschema bei Wahl der zentrierten Basis $\{u_1^2, u_1u_2 \ldots, u_1u_k\}$ betrachtet. In der Arbeit von Shamir (1993b) wird zwar geraten, keine Basen mit nichttrivialem größten gemeinsamen Teiler zu verwenden, in Hinblick auf die bereits vorgestellten Angriffe ist jedoch auch die zentrierte Basis von Interesse: Wir zeigen, wie die Eigenschaft des nichttrivialen größten gemeinsamen Teilers ausgenutzt werden kann, um den geheimen Schlüssel zu finden.

7.1 Mathematische Hilfsmittel

Satz 7.1 (siehe Becker und Weispfennig (1993), Corollary 2.71) Sei K ein Körper, $n \in \mathbb{N}$. Dann gibt es einen Algorithmus, der den größten gemeinsamen Teiler zweier Polynome aus $K[x_1, \ldots, x_n]$ bestimmt.

7.2 Rekonstruktion des geheimen Schlüssels

Das Verfahren wird für ein beliebiges $k \geq 3$ beschrieben. Alle Berechnungen werden zunächst unter der Voraussetzung ausgeführt, daß der Modul n eine Primzahl ist. Für den Angriff seien die nachfolgenden Bedingungen erfüllt.

Nicht-Entartungsbedingungen 7.2

Sei A die Variablentransformation des geheimen Schlüssels.
Forderung: In der ersten Spalte von A seien alle Einträge von Null verschieden.

7.2.1 Struktur der Formenmatrizen

Lemma 7.3 Sei $k \geq 3$. Jede Linearkombination der Basiselemente $u_1^2, u_1u_2 \ldots, u_1u_k$ ist eine quadratische Form vom Rang kleiner oder gleich 2.

Beweis Die Formenmatrix einer Linearkombination $\sum_{i=1}^{k} a_i u_1 u_i$ mit $a_1, \ldots, a_k \in \mathbb{Z}_n$ lautet

$$\frac{1}{2}\begin{pmatrix} 2a_1 & a_2 & \cdots & a_k \\ a_2 & & & \\ \vdots & & 0 & \\ a_k & & & \end{pmatrix}.$$

Der Rang dieser Matrix ist kleiner oder gleich 2. □

Seien $v_1, \ldots, v_{k-1}$ die durch (4.2) definierten Polynome des öffentlichen Schlüssels. Jedes dieser Polynome ist eine Linearkombination der Basiselemente $u_1^2, u_1u_2 \ldots, u_1u_k$. Es folgt

Lemma 7.4 Die Polynome $v_1, \ldots, v_{k-1}$ des öffentlichen Schlüssels sind quadratische Formen vom Rang kleiner oder gleich 2.

7.2.2 Charakterisierung der Variablentransformation

Sei B die geheime Matrix, die gemäß (4.2) die Linearkombinationen der Basiselemente festlegt. In den ursprünglichen Variablen $u_1, \ldots, u_k$ gilt

$$\begin{aligned} v_i &= \sum_{j=1}^{k} b_{ij} u_1 u_j \\ &= u_1 \cdot \sum_{j=1}^{k} b_{ij} u_j, \quad 1 \leq i \leq k-1. \end{aligned}$$

Der Koeffizientenvektor, der die ursprüngliche Variable u_i mit den neuen Variablen $y_1, \ldots, y_k$ verbindet, wird wie in Bezeichnung 5.15 ebenfalls mit u_i bezeichnet, $1 \leq i \leq k$.

Jedes Polynom $v_1, \ldots, v_{k-1}$ in den neuen Variablen $y_1, \ldots, y_k$ enthält als Faktor die durch den Koeffizientenvektor u_1 definierte Linearform

$$\sum_{j=1}^{k} (u_1)_j y_j = \sum_{j=1}^{k} a_{1j} y_j.$$

Die Matrix A ist hierbei die geheime Variablentransformation aus (4.1).

Da die geheimen Transformationsmatrizen A und B invertierbar sind, sind die linearen Funktionen

$$\sum_{j=1}^{k} b_{ij} u_j, \quad 1 \leq i \leq k$$

in den neuen Variablen bis auf konstante Faktoren aus $\mathbb{Z}_n$ paarweise teilerfremd. Der größte gemeinsame Teiler je zweier Polynome v_i und v_j in den neuen Variablen, $1 \leq i \neq j \leq k$, ist deshalb bis auf einen konstanten Faktor aus $\mathbb{Z}_n$ das lineare Polynom

$$\sum_{j=1}^{k} (u_1)_j y_j.$$

Die Ermittlung des größten gemeinsamen Teilers erfolgt durch Anwendung von Satz 7.1. Im nicht-entarteten Fall ist die erste Komponente des Koeffizientenvektors u_1 ungleich Null. Diese Komponente kann nach Lemma 4.7 auf 1 normiert werden. Es folgt:

Lemma 7.5 Der Koeffizientenvektor u_1 kann explizit berechnet werden.

Im Gegensatz zum Koeffizientenvektor u_1 sind die Koeffizientenvektoren $u_2, \ldots, u_k$ nicht eindeutig bestimmt.

Lemma 7.6 Seien $u'_2, \ldots, u'_k$ beliebige Vektoren aus $\mathbb{Z}_n^k$, so daß $u_1, u'_2, \ldots, u'_k$ linear unabhängig sind. Dann gilt: Die Menge der Linearkombinationen von $u_1^2, u_1u_2, \ldots, u_1u_k$ und von $u_1^2, u_1u'_2, \ldots, u_1u'_k$ sind identisch.

Beweis Es gilt

$$\text{span}(u_1, u_2, \ldots, u_k) = \text{span}(u_1, u'_2, \ldots, u'_k) = \mathbb{Z}_n^k$$

Eine Linearkombination $\sum_{i=1}^{k} a_i u_1 u_i$ mit $a_1, \ldots, a_k \in \mathbb{Z}_n$ ist auch eine Linearkombination von $u_1^2, u_1u'_2, \ldots, u_1u'_k$, denn

$$\sum_{i=1}^{k} a_i u_1 u_i = u_1(a_1 u_1 + \sum_{i=2}^{k} a_i u_i) = u_1(a'_1 u_1 + \sum_{i=2}^{k} a'_i u'_i) = a'_1 u_1^2 + \sum_{i=2}^{k} a'_i u_1 u'_i$$

mit $a'_1, \ldots, a'_k \in \mathbb{Z}_n$. Die Aussage gilt analog in der anderen Richtung. □

Aufgrund Lemma 7.6 können die Koeffizientenvektoren $u_2, \ldots, u_k$ durch die Koeffizientenvektoren $u'_2, \ldots, u'_k$ ersetzt werden.

Das nicht veröffentlichte k-te Polynom v_k kann durch das Polynom

$$v'_k = u_1^2 + \sum_{i=2}^{k} u_1 u'_i$$

ersetzt werden. Sei A' die Matrix, die aus den Zeilen $u_1, \ldots, u_k$ besteht. A' ersetzt die Variablentransformation A des geheimen Schlüssel. Wie im Fall der symmetrischen Basis kann aus der Variablentransformation A' die Matrix B' für die Linearkombinationen berechnet werden. Die beiden Matrizen A' und B' bilden ein Paar von Matrizen, die den vorgegebenen öffentlichen Schlüssel generieren. Wir haben den geheimen Schlüssel entdeckt.

7.3 Zusammengesetzte Moduln

Der Koeffizientenvektor u_1 ist bei einem zusammengesetzten Modul $n = p \cdot q$ sowohl modulo p als auch modulo q eindeutig bestimmt. Der Chinesische Restsatz überträgt die Eindeutigkeit auf die Rechnungen modulo n. Die Wahl der Koeffizientenvektoren $u_2, \ldots, u_k$ ist modulo p, modulo q und modulo n beliebig.

7.4 Sonderfälle

Die Nicht-Entartungsbedingungen 7.2 wird bei der Normierung des Koeffizientenvektors u_1 benutzt. Bei zufälliger Wahl der Transformationsmatrizen ist die Forderung mit großer Wahrscheinlichkeit erfüllt.

7.5 Beispiel

Sei $k = 5$. Wie beim Beispiel für die symmetrische und die asymmetrische Basis wird der Modul $n = p \cdot q = 7853 \cdot 8647$ verwendet, und die Transformationsmatrizen sind

$$A = \begin{pmatrix} 936 & 75 & 494 & 559 & 229 \\ 70 & 868 & 624 & 42 & 975 \\ 855 & 568 & 573 & 532 & 227 \\ 670 & 96 & 705 & 225 & 5 \\ 724 & 437 & 247 & 928 & 818 \end{pmatrix}, \quad B = \begin{pmatrix} 684 & 53 & 821 & 512 & ,509 \\ 951 & 651 & 172 & 252 & 776 \\ 468 & 610 & 618 & 892 & 293 \\ 476 & 300 & 750 & 899 & 126 \\ 365 & 404 & 502 & 863 & 190 \end{pmatrix}.$$

Um bei der Darstellung des Beispiels extrem große Zahlen zu vermeiden, werden alle weiteren Zahlen modulo p angegeben. Die symmetrischen Matrizen des öffentlichen Schlüssels lauten

$$C_1 = \begin{pmatrix} 889 & 870 & 7500 & 6889 & 3474 \\ 870 & 5747 & 7566 & 7791 & 3534 \\ 7500 & 7566 & 2464 & 5814 & 1056 \\ 6889 & 7791 & 5814 & 1084 & 5290 \\ 3474 & 3534 & 1056 & 5290 & 1975 \end{pmatrix}, \quad C_2 = \begin{pmatrix} 7354 & 6075 & 6887 & 5476 & 4275 \\ 6075 & 5035 & 5697 & 3787 & 3890 \\ 6887 & 5697 & 4797 & 6909 & 3736 \\ 5476 & 3787 & 6909 & 2103 & 4635 \\ 4275 & 3890 & 3736 & 4635 & 3019 \end{pmatrix},$$

$$C_3 = \begin{pmatrix} 772 & 556 & 4661 & 4872 & 618 \\ 556 & 1170 & 6043 & 4275 & 2959 \\ 4661 & 6043 & 2063 & 6881 & 2286 \\ 4872 & 4275 & 6881 & 5138 & 7455 \\ 618 & 2959 & 2286 & 7455 & 4984 \end{pmatrix}, \quad C_4 = \begin{pmatrix} 7287 & 1158 & 6389 & 7233 & 1742 \\ 1158 & 4112 & 1182 & 7260 & 769 \\ 6389 & 1182 & 7350 & 1746 & 5280 \\ 7233 & 7260 & 1746 & 3100 & 7327 \\ 1742 & 769 & 5280 & 7327 & 3516 \end{pmatrix}.$$

Der größte gemeinsame Teiler je zweier quadratischer Formen $v_i = y^T C_i y$, $1 \leq i \leq 4$, ergibt ein Vielfaches von u_1. Die erste Komponente von u_1 kann auf 1 normiert werden.

$$u_1 = (1, 5915, 5454, 5345, 2878)^T$$

Für die Koeffizientenvektoren $u'_2, \ldots, u'_5$ können Einheitsvektoren gewählt werden. Die Matrix A' für die Variablentransformation lautet damit

$$A' = \begin{pmatrix} 1 & 5915 & 5454 & 5345 & 2878 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Die Formenmatrix C'_5 des Polynoms v'_5 lautet

$$C'_5 = \begin{pmatrix} 1 & 1989 & 1528 & 1419 & 6805 \\ 1989 & 172 & 2044 & 5127 & 6389 \\ 1528 & 2044 & 4406 & 2767 & 2631 \\ 1419 & 5127 & 2767 & 5156 & 6921 \\ 6805 & 6389 & 2631 & 6921 & 847 \end{pmatrix}.$$

Aus den Gleichungen des öffentlichen Schlüssels und der Matrix A' ergibt sich die passende Matrix B', welche die Linearkombinationen der Basiselemente beschreibt.

$$B' = \begin{pmatrix} 889 & 37 & 537 & 4645 & 2167 \\ 7354 & 2011 & 6884 & 5222 & 6596 \\ 772 & 1391 & 6762 & 2714 & 2402 \\ 7287 & 7340 & 6395 & 2490 & 2385 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Das Paar (A', B') bildet den privaten Schlüssel.

Kapitel 8

Charakterisierung der algebraischen Basen

In diesem Kapitel werden die in Definition 4.3 eingeführten algebraischen Basen analysiert. Zunächst werden in Abschnitt 8.1 die beiden vorgestellten Signaturprotokolle in einem allgemeineren Rahmen betrachtet. Die Abschnitte 8.2 bis 8.5 charakterisieren die algebraischen Basen unabhängig von den Kryptosystemen.

8.1 Ein allgemeines Basiskonzept für die Signaturprotokolle

Es ist möglich, das Unterschriftenschema der sequentiellen Linearisierung in das Konzept der algebraischen Basen einzuordnen. Wir betrachten zunächst die Unterschiede zwischen den vorgestellen Signaturprotokollen. Anschließend beschreiben wir die Verallgemeinerungen, die für die Zusammenführung der beiden Kryptosysteme notwendig sind.

Unterschiede

Das Schema auf der Grundlage sequentieller Linearisierung:

1. Eine Unterschrift besteht aus Zuweisungen an die Variablen $x_1, \ldots, x_k$. Diese Zuweisungen ordnen jedem linearen und jedem quadratischen Polynom in $x_1, \ldots, x_k$ einen Wert aus $\mathbb{Z}_n$ zu.
2. Der geheime Schlüssel besteht aus zwei linearen Transformationen sowie einem sequentiell linearisierten Gleichungssystem.

Das Schema auf der Grundlage algebraischer Basen:

1. Eine Unterschrift besteht aus Zuweisungen an die Elemente einer algebraischen Basis für die homogenen quadratischen Polynome in $y_1, \ldots, y_k$. Diese Zuweisungen ordnen jedem homogenen quadratischen Polynom in $y_1, \ldots, y_k$ einen Wert aus $\mathbb{Z}_n$ zu.

2. Der geheime Schlüssel besteht aus zwei linearen Transformationen.

Verallgemeinerungen

1. Die Menge $\{x_1, \ldots, x_k\}$ ist eine algebraische Basis für

$F_{1,2}[x_1, \ldots, x_k] := \{f \in K[x_1, \ldots, x_k] : \text{Jeder Term von } f \text{ hat den totalen Grad 1 oder 2}\}$.

Damit liegt dem Schema der sequentiellen Linearisierung ebenfalls eine algebraische Basis zugrunde.

2. Das sequentiell linearisierte Gleichungssystem kann als eine zusätzliche nichtlineare Variablentransformation interpretiert werden. Wir gehen von einer Basis $\{z_1, \ldots, z_k\}$ aus. Die Variablen $z_1, \ldots, z_k$ werden gemäß (2.1) durch die sequentiell linearisierten Gleichungen

$$\begin{aligned} z_1 &= y_1, \\ z_i &= l_i(y_1, \ldots, y_{i-1}) \cdot y_i + q_i(y_1, \ldots, y_{i-1}), \quad 2 \leq i \leq k, \end{aligned}$$

in die Variablen $y_1, \ldots, y_k$ übergeführt.

Die Transformation ist rational umkehrbar. Mit Hilfe der ersten Gleichung läßt sich y_1 als rationale Funktion in $z_1, \ldots, z_k$ ausdrücken, mit Hilfe von

$$y_i = \frac{z_i - q_i(y_1, \ldots, y_{i-1})}{l_i(y_1, \ldots, y_{i-1})}, \quad 2 \leq i \leq k,$$

lassen sich sukzessive $y_2, \ldots, y_k$ als rational Funktion in $z_1, \ldots, z_k$ ausdrücken.

8.2 Termbasen

Nicht nur in Hinblick auf die Kryptosysteme sind algebraische Basen einfacher Struktur von besonderem Interesse. Eine algebraische Basis für $F_d[y_1, \ldots, y_k]$, in der jedes Element ein Term vom Grad d ist, bezeichnen wir im folgenden als eine **Termbasis** für $F_d[y_1, \ldots, y_k]$. Die symmetrische, die asymmetrische und die zentrierte Basis fallen in die Kategorie der Termbasen.

Definition 8.1 $T_d[y_1, \ldots, y_k]$ bezeichnet die Menge der polynomialen Terme vom Grad d in k Variablen, d.h.

$$T_d[y_1, \ldots, y_k] := \{y_{i_1} \cdot \ldots \cdot y_{i_d} : i_1, \ldots, i_d \in \{1, \ldots, k\}\}.$$

Definition 8.2 Seien $d, k \in \mathbb{N}$. Ein Element $a \in T_d[y_1, \ldots, y_k]$ heißt **Quotientenkombination** der m Elemente $a_1, \ldots, a_m \in T_d[y_1, \ldots, y_k]$, wenn a in der Form

$$a = \frac{a_{i_1} \cdot \ldots \cdot a_{i_{s+1}}}{a_{j_1} \cdot \ldots \cdot a_{j_s}} \text{ mit } s \in \mathbb{N}, \quad i_1, \ldots, i_{s+1}, j_1, \ldots, j_s \in \{1, \ldots, m\}$$

darstellbar ist.

Für die weiteren Aussagen sei ein Körper K zugrunde gelegt.

Sei G eine Termbasis für $F_d[y_1, \ldots, y_k]$. Jedes Element aus $F_d[y_1, \ldots, y_k]$ kann folglich als algebraischer Ausdruck in den Basiselementen, den Körperelementen und den vier Operationen Addition, Subtraktion, Multiplikation, restfreie Division dargestellt werden. Der folgende Satz besagt, daß jedes Element aus $T_d[y_1, \ldots, y_k]$ bereits als Quotientenkombination der Basiselemente dargestellt werden kann.

Satz 8.3 Seien $d, k \in \mathbb{N}$. Ist die Menge $G = \{g_1, \ldots, g_m\} \subseteq T_d[y_1, \ldots, y_k]$ eine Termbasis für $F_d[y_1, \ldots, y_k]$, dann ist jeder Term aus $T_d[y_1, \ldots, y_k]$ durch eine Quotientenkombination der Basiselemente darstellbar.

Leicht einzusehen ist zunächst das folgende

Fakt 8.4 Seien $d, k \in \mathbb{N}$ und $G = \{g_1, \ldots, g_m\}$ eine Termbasis für $F_d[y_1, \ldots, y_k]$. Jeder algebraische Ausdruck in den Basiselementen und den Elementen des Körpers K, in dem nur die Operationen Addition, Subtraktion, Multiplikation, restfreie Division vorkommen, läßt sich in der Form

$$\frac{p(g_1, \ldots, g_m)}{q(g_1, \ldots, g_m)} \text{ mit } p(x_1, \ldots, x_m), q(x_1, \ldots, x_m) \in K[x_1, \ldots, x_m]$$

schreiben.

Beweis (des Satzes) Sei $t \in T_d[y_1, \ldots, y_k]$ und

$$t = \frac{p(g_1, \ldots, g_m)}{q(g_1, \ldots, g_m)} \text{ mit } p(x_1, \ldots, x_m), q(x_1, \ldots, x_m) \in K[x_1, \ldots, x_m].$$

Es folgt

$$p(g_1, \ldots, g_m) = t \cdot q(g_1, \ldots, g_m).$$

Aus jedem Term $s(x_1, \ldots, x_m)$ von $q(x_1, \ldots, x_m)$ entsteht nach dem Substituieren der Basiselemente ein Polynom $s(g_1, \ldots, g_m) \in K[y_1, \ldots, y_k]$. Da G eine Termbasis ist, ist $s(g_1, \ldots, g_m)$ ein Term in $y_1, \ldots, y_k$. Folglich gibt es zu jedem Term s_1 von $q(g_1, \ldots, g_m)$ einen Term $s_1'(x_1, \ldots, x_m)$ von $q(x_1, \ldots, x_m)$ mit

$$s_1'(g_1, \ldots, g_m) = s_1.$$

Sei einer dieser Terme s_1 fest gewählt. Das Polynom $p(g_1, \ldots, g_m)$ geht aus dem Polynom $q(g_1, \ldots, g_m)$ dadurch hervor, daß jedes Monom von $q(g_1, \ldots, g_m)$ mit dem Term t multipliziert wird. Der Term $s_2 := t \cdot s_1$ ist deshalb ein Term von $p(g_1, \ldots, g_m)$. Zu dem Term s_2 gibt es einen Term $s_2'(x_1, \ldots, x_m)$ von $p(x_1, \ldots, x_m)$ mit

$$s_2'(g_1, \ldots, g_m) = s_2.$$

Es gilt

$$t = \frac{s_2}{s_1} = \frac{s_2'(g_1, \ldots, g_m)}{s_1'(g_1, \ldots, g_m)}.$$

Der Quotient

$$\frac{s_2'(g_1,\ldots,g_m)}{s_1'(g_1,\ldots,g_m)}$$

ist eine Quotientenkombination der Basiselemente. □

Satz 8.5 Für $d,k \in \mathbb{N}$ bildet die Menge

$$G = \{g_1,\ldots,g_k\} = \{y_1^d, y_1^{d-1}y_2, y_1^{d-1}y_3, \ldots, y_1^{d-1}y_k\}$$

eine Termbasis für $F_d[y_1,\ldots,y_k]$.

Beweis Im Fall $d = 1$ ist $G = \{y_1,\ldots,y_k\}$. Diese Menge bildet offenbar eine Termbasis für $F_1[y_1,\ldots,y_k]$. Im folgenden sei $d \geq 2$.

Darstellbarkeit jedes Elements aus $T_d[y_1,\ldots,y_k]$: Sei $y_{i_1}y_{i_2}\cdot\ldots\cdot y_{i_d} \in T_d[y_1,\ldots,y_k]$. Es gilt

$$y_{i_1}y_{i_2}\cdot\ldots\cdot y_{i_d} = \frac{(y_1^{d-1}y_{i_1})(y_1^{d-1}y_{i_2})\cdot\ldots\cdot(y_1^{d-1}y_{i_d})}{(y_1^d)^{d-1}}.$$

Strukturelle algebraische Unabhängigkeit: Sei p ein Polynom aus $K[x_1,\ldots,x_k]$, für das $p(g_1,\ldots,g_k)$ das Nullpolynom in $K[y_1,\ldots,y_k]$ ist. Gemäß Definition 4.2 ist zu zeigen, daß p das Nullpolynom ist.

Das Polynom p habe den totalen Grad n. Es gibt eindeutig bestimmte Polynome $p_i \in K[x_1,\ldots,x_k]$ vom totalen Grad i, $0 \leq i \leq n$, so daß

$$p(x_1,\ldots,x_k) = \sum_{i=0}^{n} p_i(x_1,\ldots,x_k).$$

Es gilt

$$\begin{aligned} p(g_1,\ldots,g_k) &= \sum_{i=0}^{n} p_i(g_1,\ldots,g_k) \\ &= \sum_{i=0}^{n} p_i(y_1^d, y_1^{d-1}y_2,\ldots,y_1^{d-1}y_k) \\ &= \sum_{i=0}^{n} (y_1^{d-1})^i \cdot p_i(y_1,\ldots,y_k) \end{aligned}$$

Das Polynom $p_i(x_1,\ldots,x_k)$ hat den totalen Grad i, das Polynom $p_i(g_1,\ldots,g_k) \in K[y_1,\ldots,y_k]$ den totalen Grad $d\cdot i$, $1 \leq i \leq n$.

Es folgt

$$\begin{aligned} p(x_1,\ldots,x_k) = 0 &\iff p_i(x_1,\ldots,x_k) = 0, \quad 1 \leq i \leq k \\ &\iff p_i(y_1,\ldots,y_k) = 0, \quad 1 \leq i \leq k \\ &\iff (y_1^{d-1})^i \cdot p_i(y_1,\ldots,y_k) = 0, \quad 1 \leq i \leq k \\ &\iff \sum_{i=0}^{n} (y_1^{d-1})^i \cdot p_i(y_1,\ldots,y_k) = 0 \\ &\iff p(g_1,\ldots,g_k) = 0 \in K[y_1,\ldots,y_k] \end{aligned}$$

Daraus folgt die Behauptung. □

Lemma 8.6 Seien $d, k \in \mathbb{N}$ und $G = \{g_1, \ldots, g_m\}$ eine Termbasis für $F_d[y_1, \ldots, y_k]$. Sei außerdem $n \in \mathbb{N}$, $n \geq 2$. Dann läßt sich jede Abbildung $f : G \to \mathbb{Z}_n^*$ eindeutig zu einer Abbildung $\tilde{f} : T_d[y_1, \ldots, y_k] \to \mathbb{Z}_n^*$ fortsetzen, so daß für alle $a \in T_d[y_1, \ldots, y_k]$ die folgende Eigenschaft erfüllt ist: Wenn a als Quotientenkombination

$$a = \frac{g_{i_1} \cdot \ldots \cdot g_{i_{s+1}}}{g_{j_1} \cdot \ldots \cdot g_{j_s}}, \quad s \in \mathbb{N}, \quad i_1, \ldots, i_{s+1}, j_1, \ldots, j_s \in \{1, \ldots, m\}$$

darstellbar ist, dann ist

$$\tilde{f}(a) = \frac{f(g_{i_1}) \cdot \ldots \cdot f(g_{i_{s+1}})}{f(g_{j_1}) \cdot \ldots \cdot f(g_{j_s})}.$$

Beweis Jedes Element $a \in T_d[y_1, \ldots, y_k]$ ist nach Satz 8.3 als Quotientenkombination der Elemente von G darstellbar. Daher ist für jedes $a \in T_d[y_1, \ldots, y_k]$ mindestens ein Wert für $\tilde{f}(a)$ definiert.

Eindeutigkeit: Seien

$$a = \frac{s_1(g_1, \ldots, g_m)}{t_1(g_1, \ldots, g_m)} \text{ und } a = \frac{s_2(g_1, \ldots, g_m)}{t_2(g_1, \ldots, g_m)}$$

mit Termen

$$s_i(x_1, \ldots, x_m), t_i(x_1, \ldots, x_m) \in K[x_1, \ldots, x_m], \quad 1 \leq i \leq 2,$$

zwei Quotientenkombinationen für a.

Fall 1: Die beiden Darstellungen für a sind äquivalent in dem Sinn, daß

$$s_1(x_1, \ldots, x_m) \cdot t_2(x_1, \ldots, x_m) - s_2(x_1, \ldots, x_m) \cdot t_1(x_1, \ldots, x_m)$$

das Nullpolynom ist. Es folgt

$$\frac{s_1(x_1, \ldots, x_m)}{t_1(x_1, \ldots, x_m)} = \frac{s_2(x_1, \ldots, x_m)}{t_2(x_1, \ldots, x_m)}$$

Nach dem Substituieren der Werte für die Basiselemente liefern die beiden algebraischen Ausdrücke den gleichen Wert für $\tilde{f}(a)$.

Fall 2: Die beiden Darstellungen für a sind nicht äquivalent, d.h.

$$s_1(x_1, \ldots, x_m) \cdot t_2(x_1, \ldots, x_m) - s_2(x_1, \ldots, x_m) \cdot t_1(x_1, \ldots, x_m)$$

ist nicht das Nullpolynom. Dann ist

$$p(x_1, \ldots, x_m) := s_1(x_1, \ldots, x_m) \cdot t_2(x_1, \ldots, x_m) - s_2(x_1, \ldots, x_m) \cdot t_1(x_1, \ldots, x_m)$$

ein Polynom aus $K[x_1, \ldots, x_m] \setminus \{0\}$, für das $p(g_1, \ldots, g_m)$ das Nullpolynom ist. Die Polynome $g_1, \ldots, g_m$ sind strukturell algebraisch abhängig. Dies ist ein Widerspruch zur Basiseigenschaft von G. □

Im nachfolgenden Satz wird die in Lemma 8.6 konstruierte Fortsetzungsfunktion ausgenutzt.

Satz 8.7 Seien $d, k \in \mathbb{N}$. Seien $G = \{g_1, \ldots, g_p\}$ und $G' = \{g'_1, \ldots, g'_q\}$ zwei Termbasen für $F_d[y_1, \ldots, y_k]$. Dann gilt $p = q$, d.h. je zwei Termbasen für $F_d[y_1, \ldots, y_k]$ haben die gleiche Mächtigkeit.

Beweis Sei $n \geq 3$, $m := |\mathbb{Z}_n^*|$. Jede Abbildung $f : G \to \mathbb{Z}_n^*$ läßt sich aufgrund Lemma 8.6 eindeutig zu der beschriebenen Abbildung $\tilde{f} : T_d[y_1, \ldots, y_k] \to \mathbb{Z}_n^*$ fortsetzen. Insbesondere sind bei dieser Fortsetzung Werte für die Elemente von G' bestimmt. Wir betrachten nun die hierdurch induzierte Abbildung $g : (\mathbb{Z}_n^*)^p \to (\mathbb{Z}_n^*)^q$, die die Belegungen der Elemente von G auf die Belegungen der Elemente von G' abbildet.

Behauptung g ist injektiv.

Jedes Element von G ist als Quotientenkombination der Basis G' darstellbar, d.h. es gilt für jedes $l \in \{1, \ldots, p\}$:

$$g_l = \frac{g'_{i_1} \cdot \ldots \cdot g'_{i_{s+1}}}{g'_{j_1} \cdot \ldots \cdot g'_{j_s}}, \quad s \in \mathbb{N}, \quad i_1, \ldots, i_{s+1}, j_1, \ldots, j_s \in \{1, \ldots, q\}.$$

Wir nehmen an, daß die Abbildung g nicht injektiv sei. Dann gibt es zwei verschiedene Belegungen für $(g_1, \ldots, g_p)$, für die die resultierende Belegung für $(g'_1, \ldots, g'_q)$ identisch ist. Da die Werte für $g_1, \ldots, g_p$ jedoch nach Lemma 8.6 eindeutig durch die Werte für $g'_1, \ldots, g'_q$ bestimmt sind, ist dies ein Widerspruch. Die Behauptung ist damit bewiesen.

Aus der Injektivität der Abbildung folgt $m^q \geq m^p$, und da $m \geq 2$ auch $|G| \leq |G'|$. Aus Symmetriegründen gilt analog $|G'| \leq |G|$ und damit $|G| = |G'|$. □

Korollar 8.8 Seien $d, k \in \mathbb{N}$. Jede Termbasis für $F_d[y_1, \ldots, y_k]$ besteht aus genau k Elementen.

Beweis Die Basis für $F_d[y_1, \ldots, y_k]$ aus Satz 8.5 hat die Mächtigkeit k. Die Aussage des Korollars folgt damit unmittelbar aus Satz 8.7. □

8.3 Quadratische Terme

Satz 8.9 Sei $k \in \mathbb{N}$ und $G = \{y_1y_2, y_2y_3, \ldots, y_ky_1\}$. G ist genau dann eine Termbasis für $F_2[y_1, \ldots, y_k]$, wenn k ungerade ist.

Beweis *Fall k gerade:* Um zu prüfen, welche Elemente von $T_d[y_1, \ldots, y_k]$ mit Hilfe von G darstellbar sind, genügt es nach Satz 8.3, die Quotientenkombinationen zu betrachten. Für jeden Term $y_iy_j \in G$ gilt: $i + j$ ist ungerade. Diese Eigenschaft bleibt bei jeder Quotientenkombination der Basiselemente erhalten. Terme der Form y_iy_j mit $i+j$ gerade sind nicht darstellbar.

Fall k ungerade: Dieser Teil der Aussage wurde bei der Einführung der symmetrischen Basis in Satz 4.5 bewiesen. □

Definition 8.10 Sei $k \in \mathbb{N}$ und $G = \{g_1, \ldots, g_k\} \subseteq T_2[y_1, \ldots, y_k]$. Jede Variable $y_1, \ldots, y_k$ komme genau zweimal in G vor. Eine Permutation

$$\pi = \begin{pmatrix} 1 & 2 & \ldots & k \\ j_1 & j_2 & \ldots & j_k \end{pmatrix}$$

heißt von G **induziert**, wenn gilt:

$$G = \{y_1 y_{j_1}, y_2 y_{j_2}, \ldots, y_k y_{j_k}\}.$$

Es gibt im allgemeinen mehrere Permutationen, die von G induziert werden. Jede dieser Permutationen besteht aus gleich vielen Zyklen.

Satz 8.11 Sei $k \in \mathbb{N}$ und $G = \{g_1, \ldots, g_k\} \subseteq T_2[y_1, \ldots, y_k]$. Jede Variable $y_1, \ldots, y_k$ komme genau zweimal in G vor. G ist genau dann eine Termbasis für $F_2[y_1, \ldots, y_k]$, wenn k ungerade ist und die durch G induzierten Permutationen aus genau einem Zyklus bestehen. Wir sprechen in diesem Fall von einer **zyklischen Basis**.

Man beachte, daß die symmetrische Basis $\{y_1y_2, y_2y_3, \ldots, y_ky_1\}$, k ungerade, eine spezielle zyklische Basis ist.

Beweis *Fall 1: Die von G induzierten Permutationen bestehen aus genau einem Zyklus.* Dann ist G identisch mit der Menge $\{y_1y_2, y_2y_3, \ldots, y_ky_1\}$ bis auf Vertauschung der Variablenbezeichnungen. Die Aussage folgt aus Satz 8.9.

Fall 2: Die von G induzierten Permutationen bestehen aus mehr als einem Zyklus. Es gibt zwei disjunkte, nichtleere Teilmengen A und B von $\{y_1, \ldots, y_k\}$, so daß in jedem Element aus G entweder nur Variablen aus A oder nur Variablen aus B auftreten. Jede Quotientenkombination

$$\frac{g_{i_1} \cdot \ldots \cdot g_{i_{s+1}}}{g_{j_1} \cdot \ldots \cdot g_{j_s}}, \quad s \in \mathbb{N}, \quad i_1, \ldots, i_{s+1}, j_1, \ldots, j_s \in \{1, \ldots, k\}$$

von Elementen aus G enthält eine gerade Anzahl von Variablen aus A und eine gerade Anzahl von Variablen aus B. Folglich lassen sich die Terme y_iy_j mit $y_i \in A$, $y_j \in B$ nicht generieren. □

Mit dem nachstehend aufgeführten Algorithmus 8.12 kann die Basiseigenschaft einer Termbasis für die homogenen quadratischen Polynome überprüft werden.

Korrektheit (von Algorithmus 8.12) Der Algorithmus terminiert, da bei jedem rekursiven Aufruf die Größe von G um 1 verringert wird.

Wenn $G \setminus \{g_j\}$ für $g_j = y_iy_l$, $l \neq i$, eine Termbasis bzgl. der verkleinerten Variablenmenge $\{y_1, \ldots, y_{i-1}, y_{i+1}, \ldots, y_k\}$ ist, dann ist G wegen

$$y_iy_m = \frac{y_iy_l \cdot y_ly_m}{y_l^2}, \quad m \in \{1, \ldots, k\}$$

Algorithmus 8.12 [Basistest für die homogenen quadratischen Polynome]

Eingabe: Variablen $y_1, \ldots, y_k$, $G = \{g_1, \ldots, g_k\} \subseteq T_2[y_1, \ldots, y_k]$
Ausgabe: $ret \in \{$**true, false**$\}$, so daß $ret =$ **true** $\iff$ G ist eine Termbasis für $F_2[y_1, \ldots, y_k]$

Wenn eine Variable y_i nur einmal in G auftritt (in dem Element g_j)
    Wende den Algorithmus auf $G \setminus \{g_j\}$ und die $k-1$ Variablen
    $y_1, \ldots, y_{i-1}, y_{i+1}, \ldots, y_k$ an, und erhalte dabei den Rückgabewert ret'.
    return (ret')
Sonst (d.h. jede Variable tritt genau zweimal auf)
    Wenn $|G|$ ungerade ist und in den durch G induzierten Permutationen
    kein echter Unterzyklus auftritt
        return (**true**)
    Sonst return (**false**)

---

ein algebraisches Erzeugendensystem für $F_2[y_1, \ldots, y_k]$. Die strukturelle algebraische Unabhängigkeit von G ist klar, da die Variable y_i in $G \setminus \{g_j\}$ nicht vorkommt. Es folgt die Basiseigenschaft von G.

Sei andererseits G eine Basis für $F_2[y_1, \ldots, y_k]$, die Variable y_i trete nur im Element g_j auf. Jeder Term $y_j y_l$, $1 \leq j, l \leq k$, $j, l \neq i$ kann als Quotientenkombination der Elemente von G dargestellt werden. In jeder dieser Kombinationen tritt die Variable y_i genauso oft im Zähler wie im Nenner auf. Da g_j das einzige Element in G ist, in dem die Variable y_i vorkommt, wird g_j bei den Kombinationen nicht benötigt. Es folgt, daß die Menge $G \setminus \{g_j\}$ eine Termbasis für $F_2[y_1, \ldots, y_{i-1}, y_{i+1}, \ldots, y_k]$ ist.

Die Korrektheit für Fall, daß jede Variable genau zweimal auftritt, folgt aus Satz 8.11. □

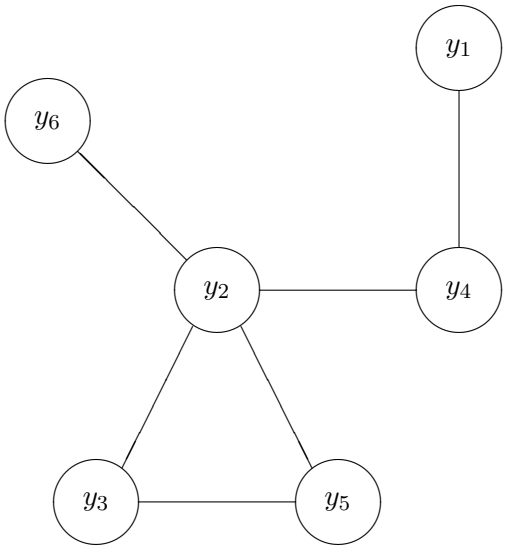
Ausgehend von dem Algorithmus zur Überprüfung der Basiseigenschaft kann die Struktur der Termbasen für die quadratischen Polynome charakterisiert werden. Jede Termbasis G besteht aus einem **zyklischen Kern** der ungeraden Größe $l \in \{1 \ldots, k\}$, d.h. G enthält eine zyklische Basis für eine l-elementige Teilmenge der Variablen. Zu diesem zyklischen Kern kommen sukzessive **Erweiterungselemente** wie folgt hinzu: Wähle jeweils zwei Variablen y_i und y_j, von denen genau eine bereits in der bisherigen Menge vorkommt, und füge $y_i y_j$ zu der Menge hinzu.

Eine gute Übersicht über die Struktur einer Termbasis vom Grad 2 erhält man durch eine graphische Darstellung. Die Variablen bilden die Knoten eines Graphen. Die Basiselemente werden durch ungerichtete Kanten zwischen zwei Knoten darstellt. In den Abbildungen 8.2 und 8.3 sind die Strukturen der symmetrischen, der asymmetrischen und der zentrierten Basis dargestellt. Bei der symmetrischen Basis besteht der zyklische Kern aus allen Basiselementen, bei der asymmetrischen und der zentrierten Basis nur aus dem Element

y_1^2.

Beispiel 8.13 Sei $G = \{y_1y_4, y_2y_3, y_2y_4, y_2y_5, y_2y_6, y_3y_5\}$. Eine mögliche Reihenfolge, in der Algorithmus 8.12 die Elemente entfernt, ist y_1y_4, y_2y_4, y_2y_6. Die drei Elemente y_2y_3, y_2y_5, y_3y_5 bilden den zyklischen Kern. In Abbildung 8.1 ist die Struktur der Basis graphisch dargestellt.

Abbildung 8.1: Struktur der Beispielbasis



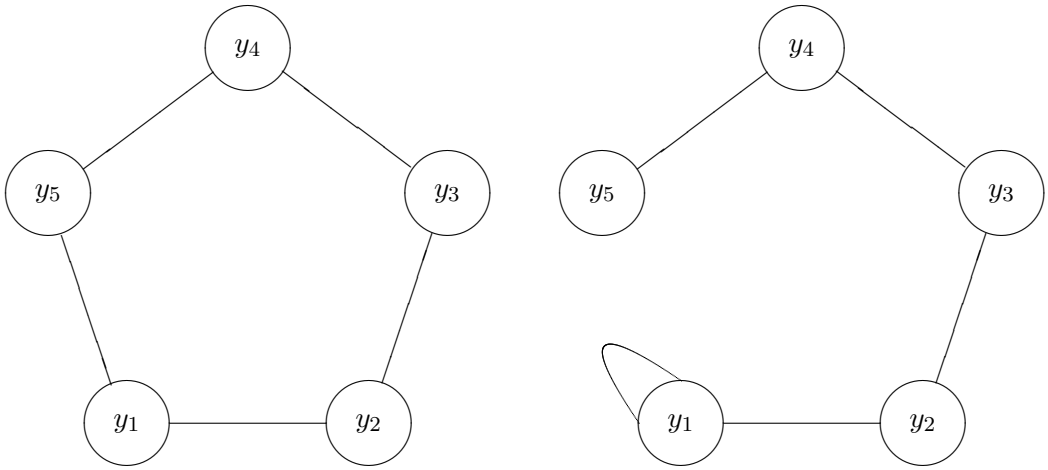
In Hinblick auf die Graphendarstellung kann man die Termbasen für die homogenen quadratischen Polynome wie folgt charakterisieren:

Satz 8.14 Sei $k \in \mathbb{N}$ und $G = \{g_1, \ldots, g_k\} \subseteq T_2[y_1, \ldots, y_k]$. G ist genau dann eine Termbasis für $F_2[y_1, \ldots, y_k]$, wenn für die Darstellung von G als Graph die folgenden Eigenschaften gelten:

- Der Graph ist zusammenhängend.
- Der Graph hat genau einen Zyklus.
- Der Zyklus hat eine ungerade Länge.

Beweis Die Eigenschaften 2 und 3 sind äquivalent dazu, daß G einen zyklischen Kern ungerader Länge besitzt. Auf dieser Grundlage ist Eigenschaft 1 äquivalent dazu, daß die Elemente, die nicht Bestandteil des zyklischen Kerns sind, Erweiterungselemente sind. □

Abbildung 8.2: Struktur der symmetrischen und der asymmetrischen Basis im Fall $k = 5$



Bemerkung 8.15 Ein zusammenhängender, azyklischer, ungerichteter Graph mit k Knoten ist ein Baum. Der Baum besteht aus genau $k-1$ Kanten. Folglich besteht ein zusammenhängender, ungerichteter Graph mit k Knoten und genau einem Zyklus aus genau k Kanten.

8.4 Kubische Terme

Wir wollen einige algebraische Erzeugendensysteme für die homogenen kubischen Polynome zusammenstellen.

Satz 8.16 Für $k \in \mathbb{N}$ gilt:

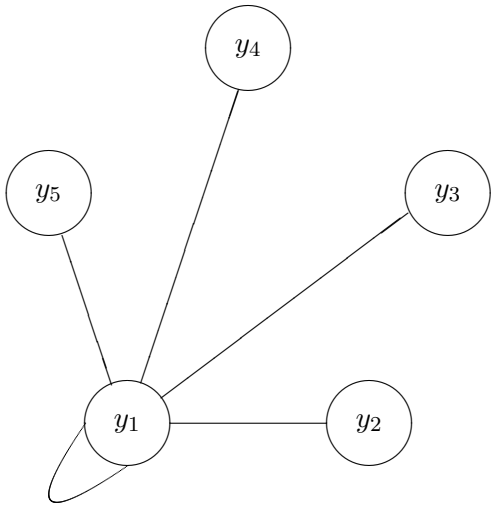
1. $\{y_1^3, y_1^2y_2, y_1^2y_3, \ldots, y_1^2y_k\}$ ist ein algebraisches Erzeugendensystem für $F_3[y_1, \ldots, y_k]$.

2. Wenn k kein Vielfaches von 3 ist, bildet $\{y_1^3, y_1y_2y_3, y_2y_3y_4, \ldots, y_{k-1}y_ky_1\}$ ein algebraisches Erzeugendensystem für $F_3[y_1, \ldots, y_k]$, $k \geq 4$.

3. Wenn k kein Vielfaches von 3 ist, bildet $\{y_1y_2y_3, y_2y_3y_4, \ldots, y_ky_1y_2\}$ ein algebraisches Erzeugendensystem für $F_3[y_1, \ldots, y_k]$, $k \geq 4$.

   Die drei Basen können in Analogie zu den Basen vom Grad 2 als zentriertes, asymmetrisches und symmetrisches Erzeugendensystem bezeichnet werden.

Abbildung 8.3: Struktur der zentrierten Basis im Fall $k = 5$



Beweis 1. Dies ist ein Spezialfall der allgemeinen Basis aus Satz 8.5. Es gilt die Darstellung

$$y_i y_j y_l = \frac{(y_1^2 y_i)(y_1^2 y_j)(y_1^2 y_l)}{(y_1^3)^2}, \quad 1 \leq i, j, l \leq k.$$

2. Wir betrachten den Fall $k = 3h + 1$, $h \in \mathbb{N}$. Der Fall $k = 3h + 2$ verläuft analog. Zunächst können mittels

$$y_{i+3}^3 = \frac{y_i^3 (y_{i+1} y_{i+2} y_{i+3})^3}{(y_i y_{i+1} y_{i+2})^3}$$

sukzessive die Elemente $y_4^3, y_7^3, \ldots, y_k^3$ dargestellt werden. Weiter ist

$$y_{k-1}^3 = \frac{(y_{k-1} y_k y_1)^3}{y_1^3 y_k^3}.$$

Nun werden durch

$$y_i^3 = \frac{y_{i+3}^3 (y_i y_{i+1} y_{i+2})^3}{(y_{i+1} y_{i+2} y_{i+3})^3}$$

rückwärts die Elemente $y_{k-4}^3, y_{k-7}^3, \ldots, y_3^3$ dargestellt. Die Elemente $y_2^3, y_5^3, \ldots, y_{k-2}^3$ können dann durch

$$y_i^3 = \frac{(y_i y_{i+1} y_{i+2})^3}{y_{i+1}^3 y_{i+2}^3}$$

dargestellt werden. Damit sind alle reinen Kuben dargestellt. Als nächstes werden die Elemente der Form $y_1^2 y_i$ erzeugt. Zunächst mittels

$$y_1^2 y_{i+3} = \frac{(y_1^2 y_i)(y_{i+1} y_{i+2} y_{i+3})}{y_i y_{i+1} y_{i+2}}$$

die Terme $y_1^2y_4, y_1^2y_7, \ldots, y_1^2y_k$, dann mittels

$$y_1^2y_{k-1} = \frac{y_1^3(y_{k-1}y_ky_1)}{y_1^2y_k}$$

der Term $y_1^2y_{k-1}$ und anschließend rückwärts die Terme $y_1^2y_{k-4}, y_1^2y_{k-7}, \ldots, y_1^2y_3$. Mit Hilfe von

$$y_1^2y_2 = \frac{y_1^3(y_1y_2y_3)}{y_1^2y_3}$$

wird $y_1^2y_2$ dargestellt. Schließlich können in aufsteigender Reihenfolge $y_1^2y_5$, $y_1^2y_8, \ldots$, $y_1^2y_{k-2}$ dargestellt werden. Damit sind alle Elemente des zentrierten Erzeugendensystems generiert worden. Es können folglich alle Elemente von $F_3[y_1, \ldots, y_k]$ erzeugt werden.

3. Wir betrachten den Fall $k = 3h+1$, $h \in \mathbb{N}$. Der Fall $k = 3h+2$ verläuft analog. Wenn y_1^3 dargestellt werden kann, können alle Elemente des asymmetrischen Erzeugendensystems erzeugt werden. y_1^3 läßt sich durch

$$y_1^3 = \frac{(y_1y_2y_3)(y_2y_3y_4)\cdot\ldots\cdot(y_{k-1}y_ky_1)(y_ky_1y_2)}{(y_2y_3y_4)^3(y_5y_6y_7)^3\cdot\ldots\cdot(y_{k-2}y_{k-1}y_k)^3}$$

generieren. □

Leider läßt sich der Basistest für die homogenen quadratischen Polynome nicht auf den Fall der kubischen Polynome übertragen. Die Idee mit den Erweiterungselementen funktioniert jedoch weiterhin und liefert damit auch bei den Kuben Informationen über die Struktur der Basen.

Satz 8.17 Sei $k \in \mathbb{N}$ und $G = \{g_1, \ldots, g_k\} \subseteq T_3[y_1, \ldots, y_k]$. Tritt eine Variable y_i nur einmal in G auf, und zwar im Element g_j, dann gilt: G ist genau dann eine Basis für $F_3[y_1, \ldots, y_k]$, wenn $G \setminus \{g_j\}$ eine Basis für $F_3[y_1, \ldots, y_{i-1}, y_{i+1}, \ldots, y_k]$ ist.

Beweis Wenn G eine Basis für $F_3[y_1, \ldots, y_k]$ ist, ist die Menge $G \setminus \{g_j\}$ eine Basis für die kubischen Polynome der $k-1$ Variablen. Die Argumentation erfolgt analog zur Betrachtung der quadratischen Polynome in Algorithmus 8.12.

Wenn die verkleinerte Menge eine Basis für die Kuben der $k-1$ Variablen $y_1, \ldots, y_{i-1}$, $y_{i+1}, \ldots, y_k$ ist und y_i nur im kubischen Term $y_iy_ly_m$ mit $l, m \neq i$ auftritt, dann ist G wegen

$$\begin{aligned}
y_iy_ry_s &= \frac{(y_iy_ly_m)(y_ly_ry_s)}{(y_l^2y_m)}, \quad 1 \leq r, s \leq k, \quad r, s \neq i, \\
y_i^2y_r &= \frac{(y_iy_ly_m)^2(y_ly_my_r)}{(y_l^2y_m)(y_m^2y_l)}, \quad 1 \leq r \leq k, \quad r \neq i, \\
y_i^3 &= \frac{(y_iy_ly_m)^3}{(y_l^2y_m)(y_m^2y_l)}
\end{aligned}$$

eine Basis für $F_3[y_1, \ldots, y_k]$. □

Im Fall, daß jede Variable mindestens zweimal in der Basis auftritt, kennen wir bisher nur sehr wenige Informationen über die Struktur der Termbasen.

Ein sehr spezielles Kriterium ist:

Satz 8.18 Sei $d \in \mathbb{N}$ und $G \subseteq T_3[y_1, \ldots, y_k]$. Kann man die Menge der Variablen $\{y_1, \ldots, y_k\}$ so in zwei disjunkte, nichtleere Teilmengen A und B zerlegen, daß jedes Element entweder nur Variablen aus der Menge A oder nur aus der Menge B enthält, dann ist G keine Termbasis für $F_3[y_1, \ldots, y_k]$.

Beweis Kubische Terme, in denen sowohl Variablen aus A als auch Variablen aus B vorkommen, lassen sich nicht generieren. Die Ausführung dieser Idee erfolgt analog zur Betrachtung der quadratischen Polynome in Satz 8.11. □

Zur graphischen Darstellung der Termbasen für die kubischen Polynome werden **Hypergraphen** benötigt. Hypergraphen sind eine Verallgemeinerung von ungerichteten Graphen. Eine Kante in einem ungerichteten Graphen verbindet zwei Knoten. Im Gegensatz dazu verbindet eine **Hyperkante** in einem Hypergraphen eine beliebige Teilmenge von Knoten.

8.5 Varietäten der Termbasen vom Grad 2

Die für diesen Abschnitt relevante Theorie findet sich im Buch von Cox, Little, O'Shea (1992) in den Paragraphen 1.2, 2.4, 2.5 und 9.1.

Definition 8.19 Ein Ideal $I \subseteq K[x_1, \ldots, x_n]$ heißt ein **Monomideal** (monomial ideal), wenn es eine (ggf. unendliche) Teilmenge der Terme in $x_1, \ldots, x_k$ gibt, die das Ideal I erzeugt.

Bemerkung 8.20 1. Aus dem Lemma von Dickson (siehe Cox, Little, O'Shea (1992), Paragraph 2.4, Satz 5 oder Becker und Weispfennig (1993), Corollary 4.48, folgt, daß jedes Monomideal von endlich vielen Termen generiert wird.

2. Monomideale sind in der Theorie der Gröbnerbasen von fundamentaler Bedeutung.

Die Termbasen, die als Ausgangsbasen für die Signaturprotokolle verwendet wurden, generieren Monomideale. Wir werden Eigenschaften dieser Monomideale analysieren, um charakteristische Unterschiede zwischen den Basen aufzuzeigen.

Die Nullstellenmenge einer Menge von Polynomen wird durch die sogenannte Varietät beschrieben:

Definition 8.21 1. Sei K ein Körper, und seien $f_1, \ldots, f_s \in K[x_1, \ldots, x_n]$. Dann ist die **affine Varietät** $V(f_1, \ldots, f_s)$ der Polynome $f_1, \ldots, f_s$ definiert durch

$$V(f_1, \ldots, f_s) = \{(a_1, \ldots, a_n) \in K^n : f_i(a_1, \ldots, a_n) = 0 \text{ für alle } 1 \leq i \leq s\}.$$

2. Die **affine Varietät** eines Ideals $I \subseteq K[x_1, \ldots, x_n]$ ist definiert durch

$$V(I) = \{(a_1, \ldots, a_n) \in K^n : f(a_1, \ldots, a_n) = 0 \text{ für alle } f \in I\}.$$

Bemerkung 8.22 Wird das Ideal I von $f_1, \ldots, f_s$ erzeugt, dann gilt

$$V(I) = V(f_1, \ldots, f_s).$$

Die graphischen Darstellungen der Varietäten generieren interessante geometrische Objekte. Unter der **Dimension einer Varietät** versteht man die geometrische Dimension der Nullstellenmenge. Die allgemeine Definition der Dimension einer Varietät verwendet das Hilbertpolynom eines Ideals. Im Falle von Monomidealen haben die Nullstellenmengen eine relativ einfache Struktur. Die Dimension kann leicht berechnet werden.

Definition 8.23 Ein **Koordinaten-Unterraum** (coordinate subspace) von $K^n = \{(x_1, \ldots, x_n) : x_1, \ldots, x_n \in K\}$ ist ein Unterraum, der dadurch definiert ist, daß einige der Variablen $x_1, \ldots, x_n$ auf Null gesetzt werden.

Satz 8.24 (Cox, Little, O'Shea (1992), Paragraph 9.1, Proposition 1, Definition 2, Proposition 3) Die Varietät $V(I)$ eines Monomideals I in $K[x_1, \ldots, x_n]$ ist eine endliche Vereinigung von Koordinaten-Unterräumen. Die Dimension von $V(I)$ ist die größte der Dimensionen der Unterräume.

Die Berechnung der Dimension kann wie folgt erfolgen. Sei das Ideal I durch die Terme $t_1, \ldots, t_s$ erzeugt. Für $1 \leq j \leq s$ sei

$$M_j = \{k \in \{1, \ldots, n\} : x_k \text{ teilt den Term } t_j\}$$

die Indexmenge der Variablen, die im Term t_j auftreten. Sei

$$\mathcal{M} = \{J \subset \{1, \ldots, n\} : J \cap M_j \neq \emptyset \text{ für alle } 1 \leq j \leq s\}$$

die Menge aller Teilmengen von $\{1, \ldots, n\}$, die einen nichtleeren Schnitt mit *jeder* Teilmenge M_j haben.

Dann gilt

$$\dim V(I) = n - \min(|J| : J \in \mathcal{M}).$$

In Kurzform: Sei v die minimale Zahl an Variablen, welche auf Null gesetzt werden müssen, um alle Terme $t_1, \ldots, t_s$ zu eliminieren. Dann gilt $\dim V(I) = n - v$.

Satz 8.25 Sei $k \in \mathbb{N}$. Die Varietäten der von uns analysierten Basen für $F_2[y_1, \ldots, y_k]$ haben die folgenden Dimensionen:

1. Symmetrische Basis (k ungerade):
$$\dim V(y_1y_2, y_2y_3, \ldots, y_ky_1) = \lfloor k/2 \rfloor = (k-1)/2.$$
2. Asymmetrische Basis:
$$\dim V(y_1^2, y_1y_2, \ldots, y_{k-1}y_k) = \lfloor k/2 \rfloor.$$
3. Zentrierte Basis:
$$\dim V(y_1^2, y_1y_2, \ldots, y_1y_k) = k-1.$$

Beweis 1. Um alle Basiselemente zu eliminieren, muß je eine von zwei benachbarten Variablen y_i, y_{i+1} muß auf Null gesetzt werden. Es müssen deshalb mindestens $\lceil k/2 \rceil$ Variablen auf Null gesetzt werden. Damit gilt

$$\dim V(y_1y_2, y_2y_3, \ldots, y_ky_1) = k - \lceil k/2 \rceil = \lfloor k/2 \rfloor = (k-1)/2.$$

2. Da y_1^2 ein Basiselement ist, muß die Variable y_1 auf Null gesetzt werden. Setzt man die folgenden Variablen auf Null, dann verschwindet jedes Basiselement:

$$\begin{aligned} &\{y_1, y_3, \ldots, y_k\} \text{ im Fall } k \text{ ungerade} \\ \text{bzw.} \quad &\{y_1, y_3, \ldots, y_{k-1}\} \text{ im Fall } k \text{ gerade.} \end{aligned}$$

Die angegebene Variablenmenge hat minimale Größe. Es folgt

$$\dim V(y_1^2, y_1y_2, \ldots, y_{k-1}y_k) = k - \lceil k/2 \rceil = \lfloor k/2 \rfloor.$$

3. Es genügt, y_1 auf Null zu setzen, um alle Basiselemente zu eliminieren. Damit gilt

$$\dim V(y_1^2, y_1y_2, \ldots, y_1y_k) = k-1.$$

□

Satz 8.26 Sei $k \in \mathbb{N}$ und G eine Termbasis für $F_2[y_1, \ldots, y_k]$. Die Dimension der Varietät von G ist mindestens $\lfloor k/2 \rfloor$.

Beweis Die Größe des zyklischen Kerns von G sei mit l bezeichnet. O.B.d.A. sei angenommen, daß der zyklische Kern aus den Elementen $y_1y_2, y_2y_3, \ldots, y_ly_1$ gebildet wird. Betrachte den Graphen, der der Basis zugeordnet ist. Jeder Knoten y_i ist Wurzel eines (eventuell einelementigen) Baumes B_i, der durch die mit dem Knoten y_i verbundenen Erweiterungselemente definiert wird, $1 \leq i \leq l$.

Für $i \in \{1, \ldots, l\}$ sei V_i die Menge der Variablen (inklusive y_i) im Baum B_i und m_i die Mächtigkeit von V_i. Mit diesen Bezeichnungen gilt $\sum_{i=1}^{l} m_i = k$.

Für $i \in \{1, \ldots, l\}$ lassen sich die folgenden beiden Aussagen leicht verifizieren.

1. Es genügt, $\lfloor m_i/2 \rfloor$ Variablen aus V_i auf Null zu setzen, um alle durch die Kanten von B_i definierten Terme zu eliminieren.

2. Wenn unter den auf Null gesetzten Variablen die Variable y_i sein soll, dann gilt: Es genügt, $\lceil m_i/2 \rceil$ Variablen aus V_i auf Null zu setzen, um alle durch die Kanten von B_i definierten Terme zu eliminieren.

Für eine Teilmenge I von $\{1, \ldots, l\}$ definieren wir

$$\text{odd}(I) := \{i \in I : m_i \text{ ist ungerade }\}.$$

Sei I_1 die Menge $\{1, 3, 5, \ldots, l\}$ und I_2 die Menge $\{1, 2, 4, \ldots, l-1\}$. *Mindestens eine* der beiden Mengen I_1, I_2 erfüllt die Bedingung

$$\text{odd}(I_i) \leq \text{ odd}(\{1, \ldots, l\} \setminus I_i) + 1, \quad 1 \leq i \leq 2.$$

Die Menge I_i, $1 \leq i \leq 2$, für die die Bedingung erfüllt ist, sei im folgenden mit I bezeichnet.

Auf die Variablen y_i mit $i \in \{1, \ldots, l\} \setminus I$ wird die Aussage 1 angewendet, auf die Variablen y_i mit $i \in I$ die Aussage 2. Die dadurch auf Null gesetzten Variablen eliminieren offensichtlich alle Elemente der Termbasis G.

Es bleibt zu zeigen: Die Anzahl der auf Null gesetzten Variablen ist kleiner oder gleich $\lceil k/2 \rceil$.

Für die Anzahl A der auf Null gesetzten Variablen gilt

$$\begin{aligned} A &\leq \sum_{i \in I} \lceil m_i/2 \rceil + \sum_{i \in \{1,\ldots,l\} \setminus I} \lfloor m_i/2 \rfloor \\ &= k/2 + 1/2 \text{ odd}(I) - 1/2 \text{ odd}(\{1, \ldots, l\} \setminus I) \\ &\leq k/2 + 1/2 \end{aligned}$$

Da A ganzzahlig ist, folgt $A \leq \lceil k/2 \rceil$. Es genügt, $A \leq \lceil k/2 \rceil$ Variablen auf Null zu setzen, um alle Terme der Basis zu eliminieren. Die Dimension der Varietät ist deshalb mindestens $k - \lceil k/2 \rceil = \lfloor k/2 \rfloor$. □

Die symmetrische Basis und die asymmetrische Basis wurden von Shamir für das Signaturschema vorgeschlagen. Die Dimension der Varietät dieser Basen ist minimal. Bei der von uns weiterhin untersuchten zentrierten Basis ist die Dimension der Varietät maximal.

Schlußbemerkung

Bei den Angriffen auf die drei Basen wurden bereits die wesentlichen Aspekte für eine Implementierung der Verfahren beschrieben. Die gegenwärtig verfügbaren Computeralgebra-Systeme sollten leistungsfähig genug sein, um die Operationen auf den Polynomen in den beschriebenen Größenordnungen durchführen zu können. Für unsere Experimente stand das System MATHEMATICA (siehe WOLFRAM (1991)) zur Verfügung.

Der Modul der beschriebenen Beispiele lautet $n = 67904091$. Die Bitlänge dieser Zahl ist 27. Folgende Rechenzeiten wurden auf einer Hewlett-Packard Workstation 9000, Modell 735/50 benötigt:

Symmetrische Basis	5 Stunden
Asymmetrische Basis	10 Minuten
Zentrierte Basis	1 Minute

Für größere Bitlängen muß man die polynomiell in der Bitlänge wachsende Rechenzeit der einzelnen Operationen in $\mathbb{Z}_n$ berücksichtigen. Sehr zeitaufwendig sind im Fall der symmetrischen Basis die Operationen auf den großen Polynomen, welche vor der Konstruktion der quadratischen Gleichung vorliegen.

Ausblick

Es bleibt ein offenes Problem, kryptographisch sichere Signatuprotokolle mit niedrigem Rechenaufwand zu konstruieren. Zur Lösung dieses Problems sind die beiden folgenden Ansätze denkbar:

1. der Entwurf neuartiger Klassen von Einwegfunktionen, auf deren Grundlage ein Verfahren mit niedrigem Rechenaufwand konstruiert wird.
2. die Modifikation bestehender Signaturmechanismen in Hinblick auf eine Minimierung des Rechenaufwandes.

Für die praktische Bedeutung digitaler Unterschriften in der nahen Zukunft wird auch der rechtliche Status von entscheidender Bedeutung sein. Dieser ist zur Zeit noch nicht vollständig geklärt.

Literatur

L. Adleman, D. Estes, K. McCurley (1987). Solving Bivariate Congruences in Random Polynomial Time. Mathematics of Computation, Vol. 48, 17-28.

T. Becker, V. Weispfennig (1993). Gröbner Bases: A Computational Approach to Commutative Algebra. Graduate Texts in Mathematics 141. Springer-Verlag, New York.

E. F. Brickell, A. M. Odlyzko (1988). Cryptanalysis: A Survey of Recent Results. Proceedings of the IEEE, Vol. 76, 578-593.

I. N. Bronstein (1989). Taschenbuch der Mathematik, 24. Auflage. Verlag Harri Deutsch, Frankfurt am Main.

D. Coppersmith, J. Stern, S. Vaudenay (1993). Attacks on the Birational Permutation Signature Schemes. Proceedings of CRYPTO 93, Lecture Notes in Computer Science, Vol. 773, 435-443.

D. Cox, J. Little, D. O'Shea (1992). Ideals, Varieties and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra. Springer-Verlag, New York.

W. Diffie, M. E. Hellman (1976). New Directions in Cryptography. IEEE Transactions on Information Theory, Vol. 22, 644-654.

F. R. Gantmacher (1986). Matrizentheorie. Springer-Verlag, Berlin.

A. K. Lenstra, H. W. Lenstra, L. Lovász (1983). Factoring Polynomials with Rational Coefficients. Mathematische Annalen 261, 515-534.

National Institute of Standards and Technology (NIST) (1992). The Digital Signature Standard, Proposal and Discussion. Communications of the ACM, Vol. 35, 33-54.

H. Ong, C. P. Schnorr, A. Shamir (1984). A Fast Signature Scheme Based on Quadratic Equations. Proceedings 16th ACM Symposium Theory on Computing, 208-216.

J. M. Pollard, C. P. Schnorr (1987). An Efficient Solution to the Congruence $x^2 + ky^2 = m \pmod{n}$. IEEE Transactions on Information Theory, Vol. 33, 702-709.

R. L. Rivest (1990). Cryptography. In: J. van Leeuven (Ed.), Handbook of Theoretical Computer Science, Vol. A. Elsevier Science Publishers B. V., Amsterdam.

R. L. Rivest, A. Shamir, L. Adleman (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM, Vol. 21, 120-126.

B. Schneier (1994). Applied Cryptography. John Wiley & Sons, New York.

A. Shamir (1993a). On the Generation of Multivariate Polynomials which are Hard to Factor. Proceedings 25th ACM Symposium Theory on Computing, 796-804.

A. Shamir (1993b). Efficient Signature Schemes Based on Birational Permutations. Proceedings of CRYPTO 93, Lecture Notes in Computer Science, Vol. 773, 1-12.

S. Vaudenay (1994). Persönliche Mitteilung.

S. Wolfram (1991). Mathematica: A System for Doing Mathematics by Computer, Second Edition. Addison-Wesley, Reading, Massachusetts.