

Analyse von auf C^* basierenden Public Key Chiffren

Diplomarbeit
von
Axel Tobias Schmidt



TECHNISCHE
UNIVERSITÄT
DARMSTADT

Fachbereich Mathematik

Betreuer: Prof. Dr. J. Buchmann

30. März 2006

Erklärung

Hiermit versichere ich, dass ich meine Diplomarbeit selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe.

Darmstadt, den 30.03.2006

Axel Tobias Schmidt

Danksagung

Mein Dank gilt Prof. Dr. J. Buchmann für die Ermöglichung dieser Diplomarbeit in seiner Arbeitsgruppe. Darüber hinaus möchte ich mich ganz herzlich bei Ralf-Philipp Weinmann für die zahlreichen Gespräche und Hilfestellungen bedanken, die mir sehr geholfen haben. Ich bedanke mich auch bei Andrei Pchikine, der viele dieser Diskussionen bereicherte. Schließlich möchte ich mich bei Prof. Dr. Keimel bedanken, der sich bereit erklärte, diese Arbeit als Zweitkorrektor zu lesen.

Inhaltsverzeichnis

1	Einführung	1
1.1	Motivation	1
1.1.1	Überblick über kryptographische Systeme	1
1.1.2	Das Quantencomputer Szenario	2
1.2	Multivariate quadratische Public Key Kryptosysteme	3
1.2.1	MQ -Systeme	3
1.2.2	Umkehrbarkeit des MQ -Systems	4
1.2.3	Affin lineare Abbildungen	5
1.2.4	Die Gestalt eines MQ -Public Key Kryptosystems	5
1.3	Mathematische Grundlagen	5
1.3.1	Körpererweiterungen	5
2	Die C^*-Chiffre	9
2.1	Einleitung	9
2.2	Funktionsweise	9
2.2.1	Umkehrung des MQ -Systems bei C^*	9
2.2.2	Die Gestalt der Verschlüsselungsabbildung	10
2.2.3	Eigenschaften des C^* -Systems	11
2.2.4	Der Inhalt der Schlüssel der C^* -Chiffre	12
2.3	Beispiel	13
2.4	Sicherheitsbetrachtung von C^*	15
2.4.1	Einschränkung des Parameters λ	15
2.4.2	Patarins Angriff	17
2.5	Fazit	19
3	Die Perturbed Matsumoto Imai Chiffre	21
3.1	Einleitung	21
3.2	Funktionsweise	21
3.2.1	Die Gestalt der Störung	22
3.3	Verschlüsselung	24
3.3.1	Öffentlicher Schlüssel	24
3.3.2	Ablauf der Verschlüsselung	24
3.4	Entschlüsselung	25
3.4.1	Privater Schlüssel	25
3.4.2	Ablauf der Entschlüsselung	25
3.5	Empfohlene Parameter	27
3.6	Einfluss der Störung auf die Effizienz des Systems	27
3.7	Fazit	27

4	Angriff auf die Perturbed Matsumoto Imai Chiffre	29
4.1	Einleitung	29
4.2	Idee und Motivation	29
4.2.1	Patarins Angriff bei konstanter Störung	30
4.2.2	Klartextklassen mit konstanter Störung	31
4.2.3	Eigenschaften der Nebenklassen	33
4.2.4	Zusammenfassung	34
4.3	Kryptoanalyse	35
4.3.1	Das Differential des öffentlichen Schlüssels	35
4.3.2	Theorem 1	39
4.3.3	Theorem 2	41
4.3.4	Theorem 3	42
4.3.5	Zusammenfassung	44
4.4	Rekonstruktion von \mathcal{K}	44
4.4.1	Analyse des Testalgorithmus T	45
4.4.2	Methode 1	46
4.4.3	Methode 2	48
4.5	Durchführung des Angriffs	50
4.6	Fazit	50
5	Die PMI+ Chiffre	53
5.1	Einleitung	53
5.2	Idee	53
5.3	Funktionsweise der PMI+-Chiffre	54
5.3.1	Ver- und Entschlüsselung mit PMI+	55
5.4	Die Auswirkungen der +-Modifikation	56
5.4.1	Analyse des Defekts von $L_{\hat{P}^+,x}$	56
5.4.2	Das Markov-Modell	60
5.4.3	Wahrscheinlichkeitsverteilung des Defekts	63
5.4.4	Verallgemeinerung der Wahl von T	64
5.4.5	Abschätzung der Anzahl a nötiger +-Polynome	66
5.4.6	Analyse der Auswirkungen der +-Modifikation	66
5.5	Empfohlene Parameter	68
5.6	Die Größe der Schlüssel	68
5.6.1	Größe des öffentlichen Schlüssels	68
5.6.2	Größe des privaten Schlüssels	68
5.7	Fazit	69

Kapitel 1

Einführung

1.1 Motivation

1.1.1 Überblick über kryptographische Systeme

Kryptographische Systeme dienen der elektronischen Verschlüsselung und Signatur von Daten sowie der Realisierung weiterer Schutzziele. Sie lassen sich grundsätzlich in symmetrische und asymmetrische Systeme unterteilen.

Symmetrische Verschlüsselungsverfahren

Symmetrische Verfahren benutzen einen Schlüssel, der sowohl zu Ver- als auch zur Entschlüsselung verwendet werden kann. Die Verfahren arbeiten meist sehr effizient, bringen aber unter anderem den Nachteil des Schlüsselverteilungsproblems mit sich. Für eine erfolgreiche verschlüsselte Kommunikation müssen die Kommunikationspartner vorher den gemeinsamen Schlüssel austauschen. Dieser Vorgang stellt ein Risiko dar, da die Sicherheit des ganzen Systems auf die Geheimhaltung des Schlüssels angewiesen ist. Der Schlüsselaustausch muss also auf sehr sicherem Weg geschehen. Das Diffie-Hellmann Schlüsselaustausch-Protokoll bietet zwar hierfür eine sichere Methode, ändert aber nichts an der Tatsache, dass für jeden Kommunikationskanal ein Schlüssel ausgehandelt werden muss. Dabei steigt die Anzahl der benötigten Schlüssel und damit auch der Schlüsselaustauschvorgänge bei mehreren Kommunikationspartnern stark an. In einer Gruppe von n Personen werden beispielsweise $n(n - 1)/2$ Schlüssel benötigt, damit jeder mit jedem verschlüsselt kommunizieren kann.

Asymmetrische Verschlüsselungsverfahren

Asymmetrische Verfahren, auch Public Key Systeme genannt, lösen das Schlüsselverteilungsproblem, indem sie für Ver- und Entschlüsselung unterschiedliche Schlüssel verwenden. Einer der Schlüssel ist öffentlich für jeden zugänglich („Öffentlicher Schlüssel“), der andere ist geheim und nur seinem Besitzer bekannt („Privater Schlüssel“). Ein abgesicherter Austausch von Schlüsseln ist nicht mehr nötig. Bei der Verschlüsselung wird eine Nachricht nun vom Sender mit dem öffentlichen Schlüssel des Empfängers verschlüsselt. Dieser Schlüssel kann vorher ungesichert ausgetauscht und verteilt werden oder in öffentlichen Verzeichnissen

bereit gestellt werden. Nur der Empfänger kann die verschlüsselte Nachricht dann mit seinem privaten Schlüssel entschlüsseln. Nähere Details zu symmetrischen und asymmetrischen Verfahren lassen sich in [Buc03] nachlesen.

Grundlagen von Public Key Systemen

Public Key Systeme basieren in der Regel auf einem schweren Problem, das nicht oder nur unter sehr großem Aufwand gelöst werden kann. Dieses Problem wird genutzt, um daraus eine sogenannte Falltürfunktion zu konstruieren. Diese Funktion arbeitet in der einen Richtung einfach und effizient, während für die effiziente Umkehrung dieser Funktion das Lösen des genannten Problems nötig wäre. Praktisch gesehen ist eine Umkehrung der Funktion also nicht möglich. Allerdings wird die Funktion so konstruiert, dass sie mit Hilfe einer zusätzlichen Information doch leicht umgekehrt werden kann. Diese Information stellt im abstrakten Sinne den privaten Schlüssel dar. In der Vergangenheit wurden diverse schwere Probleme zur Konstruktion von Public Key Kryptosystemen verwendet, so zum Beispiel das Faktorisierungsproblem beim RSA Verfahren oder das Diskrete Logarithmen Problem beim El-Gamal Verfahren. Beim Faktorisierungsproblem geht es um die Schwierigkeit, das Produkt zweier großer Primzahlen wieder in seine Primfaktoren zu zerlegen. Das Diskrete Logarithmen Problem beruht auf der Schwierigkeit, die Gleichung $x^m = y$ über einem endlichen Körper zu lösen.

Public Key Verfahren arbeiten in der Regel deutlich langsamer als symmetrische Verfahren, sind aber aufgrund mehrerer Aspekte aus der modernen Kryptographie nicht mehr wegzudenken. Zu diesen Aspekten gehören unter anderem die Lösung des Schlüsselverteilungsproblems, die erst einen sinnvollen Einsatz von Kryptographie in komplexeren Kommunikationsinfrastrukturen möglich macht, und die Tatsache, dass Public Key Verfahren die Grundlage aller gängigen Verfahren zu elektronischen Signatur darstellen. Der Nachteil der geringeren Effizienz von Public Key Systemen kann unter anderem durch Kombination mit symmetrischen Verfahren in sogenannten Hybrid-Verfahren ausgeglichen werden. Hier kommen die Vorteile beider Verfahren zur Geltung.

1.1.2 Das Quantencomputer Szenario

Die gegenwärtig verwendeten Public Key Systeme bieten schon seit verhältnismäßig langer Zeit ein hohes Sicherheitsniveau, da die zugrunde liegenden schweren Probleme bisher nicht effizient, das heißt nicht in Polynomialzeit, gelöst werden konnten. Mit der Entwicklung schnellerer Computer sind zwar die Möglichkeiten der Kryptoanalyse deutlich größer geworden, entsprechend groß gewählte Parameter der Kryptosysteme gewährleisten aber dennoch einen ausreichenden Schutz. Dieser Zustand ist aber durch die Entwicklung von Quantencomputern in großer Gefahr.

Quantencomputer basieren auf einem komplexen Grundprinzip, das sich Gesetzmäßigkeiten der Quantenmechanik zu Nutze macht. So existieren nicht nur die Zustände 0 und 1 wie bei klassischen Computern, sondern auch sogenannte Superpositionen dieser Zustände. Ein Quantencomputer ist daher theoretisch in der Lage, eine große Anzahl von Operationen gleichzeitig auszuführen. Dieser Effekt wird beispielsweise vom speziell für Quantencomputer entwickelten Algorithmus von Shor ausgenutzt, um eine Zahl effizient in ihre Primfaktoren zu

zerlegen. Das Faktorisierungsproblem kann somit in Quantum-Polynomialzeit gelöst werden. Damit bietet das RSA Verfahren keine Sicherheit mehr. Noch ist die Entwicklung von Quantencomputern im Anfangsstadium, so dass derzeit noch keine großen Zahlen faktorisiert werden können. Nach Meinung einiger Experten ist es aber nur eine Frage der Zeit, bis die gegenwärtigen Standards der Public Key Kryptographie nahezu nutzlos sein werden. Es müssen daher neue Systeme entwickelt werden, die auch von Quantencomputern nicht in polynomieller Zeit gebrochen werden können.

Quantencomputer befinden sich derzeit in einer frühen Phase der Entwicklung, so dass ihre Möglichkeiten noch nicht in vollem Umfang eingeschätzt werden können. Es besteht jedoch Anlass zur Annahme, dass Quantencomputer nicht in der Lage sein werden, schwere Probleme, das heißt Probleme, die gegenwärtig höchstens in nicht-polynomieller Zeit gelöst werden können, allgemein in polynomieller Zeit zu lösen. Möglicherweise können für einige dieser Probleme spezifische Algorithmen für Quantencomputer gefunden werden, wie beispielsweise der Algorithmus von Shor für das Faktorisierungsproblem, sie werden aber vermutlich nicht allgemein gelöst werden. Somit stellt es einen aussichtsreichen Ansatz dar, neue schwere Probleme als Grundlage zur Konstruktion von Public Key Kryptosystemen zu verwenden. Das Lösen multivariater quadratischer Gleichungssysteme ist ein Kandidat für ein solches schweres Problem. In den letzten Jahren wurden diverse Public Key Kryptosysteme entwickelt, die auf multivariaten quadratischen Gleichungssystemen basieren. Sie befinden sich gegenwärtig in einer Evaluierungsphase, in der die Sicherheit und Umsetzbarkeit dieser Verfahren untersucht wird. Einige dieser neuen Systeme werden in dieser Diplomarbeit vorgestellt und analysiert.

1.2 Multivariate quadratische Public Key Kryptosysteme

1.2.1 MQ -Systeme

Das Lösen multivariater linearer Gleichungssysteme ist ein Problem, das beispielsweise durch den Algorithmus von Gauß leicht in polynomieller Zeit gelöst werden kann. Erhöht man jedoch den Grad der Polynome, so wird das Lösen der Gleichungssysteme sehr schwer. Dabei spielt der Grad keine so große Rolle, schon der quadratische Fall mit Grad 2 stellt ein schweres Problem dar. Damit bietet sich die Verwendung multivariater quadratischer Systeme als Basis für die Konstruktion von Public Key Kryptosystemen an. Es werden dazu Polynome von quadratischem Grad verwendet, da ein höherer Grad aufgrund der resultierenden größeren Anzahl von Koeffizienten nur die Größe des öffentlichen Schlüssels unnötig erhöht, nicht aber die Sicherheit nennenswert verbessert. Multivariate quadratische Systeme, kurz MQ -Systeme, werden über endlichen Körpern realisiert. Dadurch wird die Effizienz im Vergleich zu Systemen wie RSA zusätzlich erhöht. Formal lässt sich ein MQ -System folgendermaßen darstellen:

Definition 1.2.1. Sei \mathbb{F} ein endlicher Körper. Seien weiter p_1, \dots, p_m quadratische Polynome in n Unbekannten x_1, \dots, x_n mit Koeffizienten $\alpha_i, \beta_{i,j}, \gamma_{i,jk} \in \mathbb{F}$

für $i = 1, \dots, m$ und $j, k = 1, \dots, n$. Dann ist der Vektor

$$p = \begin{cases} y_1 := p_1(x_1, \dots, x_n) = \sum_{1 \leq j \leq k \leq n} \gamma_{1,jk} x_j x_k + \sum_{1 \leq j \leq n} \beta_{1,j} x_j + \alpha_1 \\ \vdots \\ y_i := p_i(x_1, \dots, x_n) = \sum_{1 \leq j \leq k \leq n} \gamma_{i,jk} x_j x_k + \sum_{1 \leq j \leq n} \beta_{i,j} x_j + \alpha_i \\ \vdots \\ y_m := p_m(x_1, \dots, x_n) = \sum_{1 \leq j \leq k \leq n} \gamma_{m,jk} x_j x_k + \sum_{1 \leq j \leq n} \beta_{m,j} x_j + \alpha_m \end{cases}$$

ein *MQ-System*.

Die Verschlüsselungsfunktion eines auf *MQ*-Systemen basierenden Public Key Kryptosystems umfasst aber aus verschiedenen Gründen noch weitere Bestandteile, die in nachfolgenden Abschnitten vorgestellt werden.

1.2.2 Umkehrbarkeit des *MQ*-Systems

Damit ein schweres Problem sinnvoll als Grundlage eines Public Key Kryptosystems verwendet werden kann, muss das Problem für den Besitzer des privaten Schlüssels und nur für ihn leicht zu lösen sein. Nur so ist gewährleistet, dass der Besitzer des privaten Schlüssels den Verschlüsselungsprozess leicht umkehren kann, während es ohne diesen Schlüssel unmöglich ist. Das bedeutet, dass bei der Konstruktion des Kryptosystems, vereinfacht gesprochen, eine Falltür eingebaut werden muss, mit deren Hilfe das schwere Problem umgangen oder gelöst werden kann. Um diese Falltür zu nutzen, muss die Kenntnis einer speziellen geheimen Information notwendig sein, so dass die Umkehrung des Systems für die Allgemeinheit nach wie vor nicht möglich ist. Diese Information stellt dann den privaten Schlüssel des Public Key Systems dar. Die Art und Weise, wie die Umkehrung des *MQ*-Systems bewerkstelligt wird, hängt natürlich von der Funktionsweise des jeweiligen Public Key Systems ab. Sie soll daher an dieser Stelle nur abstrakt am Beispiel des C^* -Systems erläutert werden.

Umkehrung des *MQ*-Systems bei C^*

Eine detaillierte Erläuterung des C^* -Systems findet sich im nächsten Kapitel. An dieser Stelle geht es nur um ein grobes Verständnis des Konzepts. Sei dazu \mathbb{F} ein endlicher Körper mit q Elementen, über dem ein *MQ*-System der Form 1.2.1 definiert ist, wobei $m = n$. Das System besteht also aus n polynomiellen Gleichungen in n Variablen. Das C^* -System nutzt nun zur Umkehrung des *MQ*-Systems die Tatsache aus, dass die Polynome dieses *MQ*-Systems speziell gewählt sind. Stellt man nämlich den \mathbb{F}^n -Vektor der n quadratischen Polynome durch eine bijektive Transformation über einem Erweiterungskörper \mathbb{E} vom Grad n von \mathbb{F} dar, so entsteht ein univariates Monom von der speziellen Gestalt

$$Y = X^{q^\lambda + 1}, \quad X, Y \in \mathbb{E}, \lambda \in \mathbb{N}.$$

Dieses Monom ist über \mathbb{E} invertierbar, denn wegen $\gcd(q^n - 1, q^\lambda + 1) = 1$ existiert $h \in \mathbb{N}$ mit

$$Y^h = (X^{q^\lambda + 1})^h = X.$$

Nach der Inversion kann wieder in den Ausgangsraum \mathbb{F}^n zurück transformiert werden. Nur der Besitzer des privaten Schlüssels hat die nötigen Informationen, um die spezielle Gestalt des MQ -Systems über \mathbb{E} zu erhalten und das System so invertieren zu können. Die Technik, einen Erweiterungskörper \mathbb{E} des Grundkörpers \mathbb{F} zu verwenden, über welchem das MQ -System eine invertierbare Gestalt hat, wird noch bei weiteren MQ -Kryptosystemen verwendet, dennoch existieren auch Systeme mit anderen Konzepten, die die Umkehrbarkeit gewährleisten.

1.2.3 Affin lineare Abbildungen

Der letzte Abschnitt macht deutlich, dass es wichtig ist, die Details der internen Struktur des MQ -Systems vor Angreifern zu verbergen, damit diese nicht die Möglichkeit erhalten, an Informationen zu gelangen, die Rückschlüsse auf die Invertierbarkeit des Systems erlauben. Zugriff auf die interne Struktur darf nur dem Besitzer des privaten Schlüssels möglich sein. Public Key Kryptosysteme, die auf MQ -Systemen aufbauen, verwenden daher zusätzliche affin lineare Abbildungen, um die Gestalt des MQ -Systems zu verschleiern. Affin lineare Abbildungen haben den Grad 1, sie verändern also den Grad der polynomiellen Abbildung bei Komposition nicht.

Definition 1.2.2. Sei M_A eine $(n \times n)$ -Matrix über \mathbb{F} und $v_A \in \mathbb{F}^n$. Dann ist

$$A(x) = M_A x + v_A, \quad x \in \mathbb{F}^n,$$

die Matrixdarstellung der affinen Abbildung A .

Bemerkung. Wenn in obiger Darstellung die Matrix M_A invertierbar ist, so operiert die Abbildung A als Permutation auf \mathbb{F}^n .

1.2.4 Die Gestalt eines MQ -Public Key Kryptosystems

Mit den vorgestellten Komponenten lässt sich nun ein abstraktes MQ -Public Key Kryptosystem aufbauen. Das MQ -System p wird nach außen durch zwei affin lineare Abbildungen S und T verschleiert. Das Ergebnis ist der öffentliche Schlüssel p_{pub} des Systems, der als Vektor die verschleierte quadratischen Polynome des MQ -Systems enthält:

$$p_{pub} = S \circ p \circ T.$$

Es existieren somit zwei MQ -Systeme: das *äußere* System p_{pub} , das den öffentlichen Schlüssel darstellt, und das *innere* System p , das sich invertieren lässt. Dabei ist nur die äußere polynomielle Abbildung p_{pub} öffentlich zugänglich, nicht aber ihre Bestandteile. Diese sind nur dem Besitzer des privaten Schlüssels p_{priv} bekannt. p_{priv} setzt sich abstrakt aus $\{S, T, p\}$ und allen zusätzlichen Informationen zusammen, die nötig sind, um p zu invertieren.

1.3 Mathematische Grundlagen

1.3.1 Körpererweiterungen

Erweiterungskörper spielen insbesondere bei den in dieser Diplomarbeit behandelten MQ -Kryptosystemen eine große Rolle. Da sie in der allgemeinen Körpertheorie und speziell auch in der Galois-Theorie von großer Bedeutung sind,

finden sich in nahezu allen Standardwerken der Algebra ausführliche Informationen zum Thema Körpererweiterung. Es sollen daher an dieser Stelle nur die grundlegenden Eigenschaften vorgestellt werden, die in den folgenden Kapiteln vielfach Anwendung finden.

Definition 1.3.1. Sei \mathbb{E} ein Körper. Eine Teilmenge $\mathbb{F} \subset \mathbb{E}$ ist ein *Unterkörper* von \mathbb{E} , falls

1. $1 \in \mathbb{F}$
2. $x, y \in \mathbb{F} \Rightarrow x + y \in \mathbb{F}, x \cdot y \in \mathbb{F}$
3. $0 \neq x \in \mathbb{F} \Rightarrow x^{-1} \in \mathbb{F}$.

Dann ist \mathbb{E} ein *Oberkörper* von \mathbb{F} und wird als *Körpererweiterung* von \mathbb{F} bezeichnet.

Erweiterungskörper \mathbb{E} als \mathbb{F} -Vektorraum

Eine entscheidende Eigenschaft von Körpererweiterungen, von der in den nächsten Kapiteln mehrfach Gebrauch gemacht werden wird, ist die Tatsache, dass der Erweiterungskörper \mathbb{E} sich als Vektorraum über \mathbb{F} auffassen lässt. Ist \mathbb{E} eine endliche Körpererweiterung von \mathbb{F} , so lässt sich jedes Element $X \in \mathbb{E}$ also darstellen als

$$X = \sum_{i=1}^n x_i \alpha_i, \quad (1.1)$$

wobei x_1, \dots, x_n aus \mathbb{F} als Koeffizienten und $\alpha_1, \dots, \alpha_n$ aus \mathbb{E} als Basiselemente des \mathbb{F} -Vektorraums \mathbb{E} aufgefasst werden. Die Dimension von \mathbb{E} als \mathbb{F} -Vektorraum,

$$[\mathbb{E} : \mathbb{F}] := \dim_{\mathbb{F}} \mathbb{E} = n,$$

ist der *Grad der Körpererweiterung*. Die Darstellung (1.1) legt nahe, wie sich der Erweiterungskörper \mathbb{E} mit \mathbb{F}^n bezüglich der Basis $\{\alpha_1, \dots, \alpha_n\}$ identifizieren lässt:

$$\begin{aligned} \mathbb{E} &\longleftrightarrow \mathbb{F}^n : \\ X = \sum_{i=1}^n x_i \alpha_i &\longleftrightarrow (x_1, \dots, x_n). \end{aligned}$$

Entsprechend ist klar, dass, falls der Körper \mathbb{F} q Elemente enthält, der Erweiterungskörper \mathbb{E} gerade q^n Elemente enthält.

Bei den in dieser Diplomarbeit betrachteten Fällen handelt es sich grundsätzlich um endliche Körpererweiterungen vom Grad n , das heißt, der Erweiterungskörper \mathbb{E} lässt sich immer als endlichdimensionaler Vektorraum über \mathbb{F} betrachten.

Weitere Eigenschaften

Endliche Körpererweiterungen sind generell algebraisch, das heißt, jedes Element $\alpha \in \mathbb{E}$ ist Nullstelle eines Polynoms $F \neq 0$ aus $\mathbb{F}[X]$. Es gilt dann folgender Zusammenhang:

Satz 1.3.1. Sei \mathbb{F} ein Körper und u ein in $\mathbb{F}[X]$ irreduzibles Polynom vom Grad n . Dann ist der Quotientenring

$$\mathbb{E} \cong \mathbb{F}[X]/(u)$$

eine Körpererweiterung von \mathbb{F} vom Grad n . In \mathbb{E} besitzt das Polynom u eine Nullstelle, nämlich die Restklasse

$$\alpha = X + u\mathbb{F}[X].$$

Die Elemente

$$1, \alpha, \alpha^2, \dots, \alpha^{n-1}$$

bilden eine Basis von \mathbb{E} über \mathbb{F} .

Bemerkung. Für die Elemente der Basis $\{\alpha_1, \dots, \alpha_n\}$ von \mathbb{E} als \mathbb{F} -Vektorraum gilt also mit den Bezeichnungen aus dem Satz

$$\alpha_i = \alpha^{i-1}, \quad i = 1, \dots, n.$$

Diese Eigenschaften kommen unter anderem bei der konkreten Durchführung eines Entschlüsselungsvorgangs in Kapitel 2 zum Tragen. Für einen Beweis des Satzes und weitere Details sei auf Standard Literatur zur Algebra verwiesen (beispielsweise [Art98]). Weitere Informationen zu MQ -Systemen und darauf basierenden Public Key Chiffren finden sich in [WP05].

Kapitel 2

Die C^* -Chiffre

2.1 Einleitung

Die C^* -Chiffre von Matsumoto und Imai (vgl. [MI88]) ist eine Realisierung eines Public Key Kryptosystems auf Basis multivariater quadratischer Gleichungssysteme über einem endlichen Körper \mathbb{F} . Als öffentlicher Schlüssel dient der Vektor P , der n quadratische Polynome über \mathbb{F} in n Unbekannten enthält. Somit kann ein Klartextvektor $x = (x_1, \dots, x_n) \in \mathbb{F}^n$ verschlüsselt werden, indem die Komponenten des Vektors in die Polynome des öffentlichen Schlüssels eingesetzt und ausgewertet werden. Das Ergebnis ist der Geheimtextvektor, der ebenfalls n Komponenten hat. Da es keine bekannte Methode gibt, um quadratische Gleichungssysteme effizient zu lösen, kann dieser Vorgang in akzeptabler Zeit nicht umgekehrt werden. Aufgrund der speziellen Konstruktion des C^* -Systems hat der Vektor der Polynome des zugrunde liegenden inneren MQ -Systems jedoch eine besondere Form, wenn er mit der Kenntnis des privaten Schlüssels über einem Erweiterungskörper \mathbb{E} des Grundkörpers \mathbb{F} betrachtet wird. Man spricht daher auch von einem MQ -System über gemischten Körpern. Über diesem Erweiterungskörper \mathbb{E} hat das innere multivariate Polynomsystem des öffentlichen Schlüssels die Gestalt eines speziellen univariaten Monoms, das sich relativ leicht invertieren lässt. Der Besitzer des privaten Schlüssels kann somit leicht aus dem Geheimtext den Klartext rekonstruieren.

2.2 Funktionsweise

2.2.1 Umkehrung des MQ -Systems bei C^*

Wie in der Einleitung erläutert, bedient sich die C^* -Chiffre zweier Körper, dem Grundkörper \mathbb{F} und dem Erweiterungskörper \mathbb{E} . Es gilt

$$[\mathbb{E} : \mathbb{F}] = n,$$

\mathbb{E} ist also eine Körpererweiterung vom Grad n des Grundkörpers \mathbb{F} . Die multivariate quadratische Abbildung des öffentlichen Schlüssels eines C^* -Systems hat die allgemeine Form

$$P : \mathbb{F}^n \rightarrow \mathbb{F}^n : x \mapsto (S \circ \tilde{P} \circ T)(x), \quad (2.1)$$

wobei S, T affin lineare, invertierbare Abbildungen sind und \tilde{P} die innere polynomielle Abbildung über \mathbb{F}^n , also das unverschleierte MQ -System, darstellt, wie in Kapitel 1 beschrieben. Dieses MQ -System ist aber bei der C^* -Chiffre speziell gewählt, so dass die Abbildung über dem Erweiterungskörper \mathbb{E} die Form eines univariaten Monoms hat, das sich aufgrund seiner speziellen Gestalt leicht invertieren lässt. Vielmehr wird das Monom bei der Konstruktion eines C^* -Systems im ersten Schritt gewählt, das MQ -System ergibt sich dann durch die Transformation des Monoms nach \mathbb{F}^n . Dieses Monom sei als geheime polynomielle Abbildung P^* über \mathbb{E} bezeichnet.

Definition 2.2.1. Sei \mathbb{E} ein Erweiterungskörper vom Grad n über dem endlichen Körper \mathbb{F} mit $q := |\mathbb{F}|$ und sei weiter $\lambda \in \mathbb{N}$ eine natürliche Zahl mit $\gcd(q^n - 1, q^\lambda + 1) = 1$. Dann hat das folgende Monom P^* über \mathbb{E} C^* -Gestalt:

$$P^*(X) = X^{q^\lambda + 1}. \quad (2.2)$$

Wie bereits erläutert, ist der entscheidende Unterschied, dass die geheime Abbildung P^* im Gegensatz zur öffentlichen Abbildung P invertierbar ist, so dass mit ihrer Hilfe Geheimitexte wieder entschlüsselt werden können. Diese Eigenschaft wird für das C^* -Polynom im folgenden Satz nachgewiesen.

Satz 2.2.1. Sei P^* von C^* -Gestalt. Dann ist P^* Permutationspolynom über \mathbb{E} und somit invertierbar bezüglich Komposition.

Beweis. Es ist $|\mathbb{E}| = q^n$. Die Ordnung der \mathbb{E} zugrunde liegenden multiplikativen Gruppe ist also $q^n - 1$. Nach dem kleinen Satz von Fermat gilt daher

$$X^{q^n - 1} = 1.$$

Wegen $\gcd(q^n - 1, q^\lambda + 1) = 1$ gilt nun:

$$\begin{aligned} \exists h \in \mathbb{N} \text{ mit } h(q^\lambda + 1) &\equiv 1 \pmod{q^n - 1} \\ \Rightarrow h(q^\lambda + 1) &= 1 + k(q^n - 1), \quad k \in \mathbb{Z} \\ \Rightarrow X^{h(q^\lambda + 1)} &= X^{1+k(q^n - 1)} = X \cdot \underbrace{(X^{q^n - 1})^k}_{=1} = X \end{aligned}$$

Also ist P^* über \mathbb{E} invertierbar und somit ein Permutationspolynom. \square

Bemerkung. Da das MQ -System \tilde{P} der C^* -Chiffre durch Transformation dieses geheimen Permutationspolynoms P^* nach \mathbb{F}^n entsteht, ist auch das MQ -System \tilde{P} bzw. P bijektiv. Jeder Geheimitext besitzt also nur einen passenden Klartext.

2.2.2 Die Gestalt der Verschlüsselungsabbildung

Es soll nun die Verschlüsselungsabbildung P so detailliert dargestellt werden, dass die geheime Abbildung P^* darin integriert ist. Das MQ -System des öffentlichen Schlüssels hat die allgemeine Form

$$P = S \circ \tilde{P} \circ T : \mathbb{F}^n \rightarrow \mathbb{F}^n,$$

wie schon in (2.1) beschrieben wurde. Um nun das Polynom P^* über dem Erweiterungskörper \mathbb{E} in einem MQ -System dieser allgemeinen Form korrekt darstellen zu können, wird noch der Isomorphismus π benötigt, der \mathbb{E} mit \mathbb{F}^n identifiziert. Sei dazu wie in Kapitel 1 $\{\alpha_1, \dots, \alpha_n\}$ die Basis des Erweiterungskörpers

\mathbb{E} , der hier als Vektorraum über dem Grundkörper \mathbb{F} betrachtet wird. Dann lässt sich π folgendermaßen darstellen:

$$\pi : \mathbb{E} \rightarrow \mathbb{F}^n \quad (2.3)$$

mit

$$\pi(a_1\alpha_1 + a_2\alpha_2 + a_3\alpha_3 + \cdots + a_n\alpha_n) = (a_1, a_2, a_3, \dots, a_n)^t.$$

Damit lässt sich nun die innere polynomielle Abbildung \tilde{P} darstellen als

$$\tilde{P} = \pi \circ P^* \circ \pi^{-1} : \mathbb{F}^n \rightarrow \mathbb{F}^n \quad (2.4)$$

und somit gilt für die öffentliche polynomielle Abbildung P schließlich

$$P = S \circ \pi \circ P^* \circ \pi^{-1} \circ T : \mathbb{F}^n \rightarrow \mathbb{F}^n. \quad (2.5)$$

In dieser detaillierten Form ist die Verschlüsselungsfunktion P nur dem Besitzer des privaten Schlüssels des System bekannt.

2.2.3 Eigenschaften des C^* -Systems

Im weiteren Verlauf werden nun noch einige Eigenschaften der C^* -Chiffre näher betrachtet.

Der Grad der Polynome des öffentlichen Schlüssels

Die C^* -Chiffre ist ein MQ -System, das bedeutet unter anderem, dass die Polynome des öffentlichen Schlüssels quadratisch über dem Grundkörper \mathbb{F} sind. Betrachtet man nun die geheime polynomielle Abbildung $P^* = X^{q^\lambda+1}$ als Ausgangspunkt eines C^* -Systems, aus der durch Transformation mittels π nach \mathbb{F}^n der Vektor \tilde{P} des inneren MQ -Systems entsteht, so ist allerdings nicht direkt ersichtlich, wieso die Polynome dieses MQ -Systems und damit auch die des verschleierte Systems P quadratisch sein sollten. P ist jedoch tatsächlich ein System multivariater quadratischer Polynome, da P^* als Produkt zweier über \mathbb{F} linearer Abbildungen betrachtet werden kann: $P^* = X^{q^\lambda+1} = X \cdot X^{q^\lambda}$, wobei X und auch X^{q^λ} \mathbb{F} -linear sind. Dies folgt, da X^{q^λ} als Potenz des Frobenius-Homomorphismus aufgefasst werden kann. Detailliert lässt sich der Zusammenhang folgendermaßen verstehen:

\mathbb{F} und \mathbb{E} sind Körper mit Mächtigkeit $|\mathbb{F}| = q$ bzw. $|\mathbb{E}| = q^n$. Nach dem kleinen Satz von Fermat gilt daher:

$$(L1) \quad (aX)^{q^\lambda} = aX^{q^\lambda} \quad \forall a \in \mathbb{F}, X \in \mathbb{E}, \lambda \in \mathbb{N}.$$

Für die Charakteristik von \mathbb{E} gilt $\text{char}(\mathbb{E}) = \text{char}(\mathbb{F}) = p$ für eine Primzahl p . Da die Mächtigkeit eines endlichen Körpers immer eine Potenz seiner Charakteristik ist, gilt daher $q = p^r$ für eine natürliche Zahl r und somit

$$(L2) \quad (X + Y)^{q^\lambda} = X^{q^\lambda} + Y^{q^\lambda} \quad \forall X, Y \in \mathbb{E}, \lambda \in \mathbb{N}.$$

Dies entspricht der Frobenius-Eigenschaft.

Aus diesen beiden Eigenschaften folgt die \mathbb{F} -Linearität des Monoms X^{q^λ} . Denn für beliebige $X \in \mathbb{E}$ gilt daher

$$X^{q^\lambda} = \left(\sum_{i=1}^n x_i \alpha_i \right)^{q^\lambda} \stackrel{(L2)}{=} \sum_{i=1}^n (x_i \alpha_i)^{q^\lambda} \stackrel{(L1)}{=} \sum_{i=1}^n x_i \alpha_i^{q^\lambda},$$

wobei für $i = 1, \dots, n$ $x_i \in \mathbb{F}$ die Koeffizienten und $\alpha_i = \alpha^{i-1} \in \mathbb{E}$ die Basiselemente von X in der Darstellung als Vektor des \mathbb{F} -Vektorraums \mathbb{E} sind. Die Terme $\alpha_i^{q^\lambda}$ sind für $i = 1, \dots, n$ in \mathbb{E} enthalten und lassen sich daher wieder als Linearkombination bezüglich der Basis $\{1, \alpha, \dots, \alpha^{n-1}\}$ mit festen Koeffizienten aus \mathbb{F} darstellen. Entscheidend ist, dass also die Koeffizienten x_i , $i = 1, \dots, n$, eines Elements $X \in \mathbb{E}$ von der Abbildung $X \rightarrow X^{q^\lambda}$ nur linear kombiniert werden. Also ist P^* und damit auch $\tilde{P} = \pi \circ P^* \circ \pi^{-1}$ sowie in Konsequenz P quadratisch über dem Grundkörper \mathbb{F} .

Die Charakteristik des Grundkörpers \mathbb{F}

Betrachtet man die Struktur von \mathbb{F} und \mathbb{E} näher, so lässt sich folgende interessante Beobachtung machen, die später noch von weitreichender Konsequenz sein wird:

Satz 2.2.2. *Sei \mathbb{F} der endliche Grundkörper eines C^* -Systems wie oben definiert. Für die Charakteristik des Körpers \mathbb{F} gilt dann*

$$\text{char}(\mathbb{F}) = 2.$$

Beweis. Es gilt nach Voraussetzung $\gcd(q^n - 1, q^\lambda + 1) = 1$. Sei q ungerade. Dann ist aber $\gcd(q^n - 1, q^\lambda + 1) \geq 2$ im Widerspruch zur Voraussetzung. Also ist q gerade. Die Charakteristik eines endlichen Körpers ist prim und die Mächtigkeit des Körpers eine Potenz der Charakteristik. Da $q = |\mathbb{F}|$ mit \mathbb{F} Körper, ist q also eine Primzahlpotenz und wegen q gerade somit eine Potenz von 2. \square

Bemerkung. Es gilt $\text{char}(\mathbb{E}) = \text{char}(\mathbb{F}) = 2$, da die Charakteristik des Erweiterungskörpers und die des Grundkörpers identisch sind.

Die im Beweis verwendete Voraussetzung $\gcd(q^n - 1, q^\lambda + 1) = 1$ ist hinreichend für die eindeutige Invertierbarkeit des C^* -Monoms P^* . Da diese Eigenschaft für ein C^* -System unerlässlich ist, kann das System also nur über Körpern der Charakteristik 2 realisiert werden. Andernfalls könnte einem Geheimtext im Allgemeinen nicht eindeutig ein Klartext zugeordnet werden. Das System müsste dann beispielsweise durch zusätzlich Berechnung von Hashwerten modifiziert werden, um den korrekten Klartext zu identifizieren, falls eine Entschlüsselung überhaupt möglich ist.

2.2.4 Der Inhalt der Schlüssel der C^* -Chiffre

Der öffentliche Schlüssel

Der öffentliche Schlüssel eines C^* -Systems muss den Vektor P des verschleierten MQ -Systems enthalten sowie die Angabe des Klartextraums \mathbb{F}^n . Aus dieser wird die Länge n der Nachrichten und der Körper \mathbb{F} , aus dem die Komponenten der Nachrichten gewählt werden müssen, ersichtlich.

Der private Schlüssel

Der private Schlüssel muss alle Informationen enthalten, die zum Entschlüsseln einer Nachricht erforderlich sind. Neben der Kenntnis des Klartextraums \mathbb{F}^n sind dies die affinen linearen Abbildungen S und T , die das innere MQ -System offenlegen. Desweiteren werden Informationen zur Darstellung des Erweiterungskörpers \mathbb{E} als \mathbb{F} -Vektorraum benötigt. Dies geschieht durch Angabe des irreduziblen Polynoms u und damit der Basis $\{1, \alpha, \dots, \alpha^{n-1}\}$, woraus sich auch der Isomorphismus π ergibt, der zwischen \mathbb{E} und \mathbb{F}^n übersetzt (vgl. Kapitel 1). Schließlich wird noch das geheime C^* -Polynom P^* , genauer der Wert λ , benötigt.

2.3 Beispiel

Das folgende Beispiel zeigt, wie man eine Nachricht m mit dem öffentlichen Schlüssel P verschlüsselt und wie der resultierende Geheimtext c anschließend mit Hilfe des privaten Schlüssels (S, P^*, T, u) wieder entschlüsselt werden kann. Dabei werden folgende Werte verwendet:

- Grundkörper $\mathbb{F} = \text{GF}(2)$, also $q = |\mathbb{F}| = 2$.
- Erweiterungskörper $\mathbb{E} = \text{GF}(8)$, also Erweiterungsgrad $n = [\mathbb{E} : \mathbb{F}] = 3$, erzeugt vom Minimalpolynom

$$u(X) = X^3 + X + 1.$$

$u(X)$ ist irreduzibel in $\mathbb{F}[X]$ und hat in \mathbb{E} die Nullstelle

$$\alpha = X + u\mathbb{F}[X].$$

\mathbb{E} lässt sich also als \mathbb{F} -Vektorraum mit der Basis $\{1, \alpha, \alpha^2\}$ betrachten und es gilt $\mathbb{E} = \mathbb{F}[\alpha] \cong \mathbb{F}[X]/(u)$ (vgl. Kapitel 1).

- Die affinen Abbildungen

$$S : \mathbb{F}^3 \rightarrow \mathbb{F}^3 : x \mapsto M_S x + v_S,$$

$$T : \mathbb{F}^3 \rightarrow \mathbb{F}^3 : x \mapsto M_T x + v_T$$

mit

$$M_S = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}, v_S = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, M_T = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, v_T = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}.$$

Für die Inversen ergibt sich

$$M_S^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, M_T^{-1} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

- Um für die geheime Polynomabbildung P^* die erforderliche Bedingung $\gcd(q^n - 1, q^\lambda + 1) = 1$ zu erfüllen, wähle $\lambda = 2$. Damit ist

$$P^*(X) = X^5.$$

Für die inverse Abbildung $(P^*)^{-1}(X) = X^h$ ergibt sich damit wegen $h(q^\lambda + 1) \equiv 1 \pmod{q^n - 1}$ der Wert $h = 3$, also

$$(P^*)^{-1}(X) = X^3.$$

- Für den öffentlichen Schlüssel gilt $P = S \circ \pi \circ P^* \circ \pi^{-1} \circ T$ mit der Transformation π wie in (2.5) bzw. (2.3) definiert. Mit obigen Werten ergibt sich für eine Nachricht $x = (x_1, x_2, x_3)^t \in \mathbb{F}^3$ die quadratische Polynomabbildung

$$P((x_1, x_2, x_3)^t) = \begin{pmatrix} x_1 + x_2 + x_3 + x_1x_3 + 1 \\ x_1 + x_1x_2 + x_2x_3 + 1 \\ x_1 + x_3 + x_2x_3 \end{pmatrix}.$$

Verschlüsselung

Um den Klartext $m = (1, 0, 0)^t \in \mathbb{F}^3$ zu verschlüsseln, wird $P(m)$ berechnet:

$$c = P((1, 0, 0)^t) = \begin{pmatrix} 1 + 0 + 0 + 1 \cdot 0 + 1 \\ 1 + 1 \cdot 0 + 0 \cdot 0 + 1 \\ 1 + 0 + 0 \cdot 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}.$$

Der entsprechende Geheimtext c ist also $(0, 0, 1)^t$.

Entschlüsselung

Um den Geheimtext c wieder zu entschlüsseln, muss P mit Hilfe des privaten Schlüssels (S, P^*, T, u) invertiert werden. Es gilt

$$m = P^{-1}(c) = (T^{-1} \circ \pi \circ (P^*)^{-1} \circ \pi^{-1} \circ S^{-1})(c). \quad (2.6)$$

Die Entschlüsselung bedarf also mehrerer Schritte:

- (i) Zuerst wird die inverse affine Abbildung S^{-1} angewendet:

$$S^{-1}(c) = M_S^{-1}(c - v_S) = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \left[\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} - \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \right] = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}.$$

- (ii) Nun wird die Transformation π^{-1} angewendet:

$$\pi^{-1}((1, 1, 0)^t) = 1 + \alpha.$$

- (iii) Als nächstes kann nun die inverse Polynomabbildung $(P^*)^{-1}$ angewendet werden. Dabei wird von den im vorangegangenen Abschnitt auf S.11 erwähnten Zusammenhängen (L1) und (L2) Gebrauch gemacht:

$$\begin{aligned} (P^*)^{-1}(1 + \alpha) &= (1 + \alpha)^3 = (1 + \alpha)(1 + \alpha)^2 = \\ &= (1 + \alpha)(1 + \alpha^2) = 1 + \alpha^2 + \alpha + \alpha^3 = \dots \end{aligned}$$

Nun muss das Ergebnis wieder bezüglich der Basis $\{1, \alpha, \alpha^2\}$ dargestellt werden, damit sich die Transformation π sinnvoll anwenden lässt. Dazu müssen die höheren α -Potenzen in \mathbb{E} modulo des Minimalpolynoms u reduziert werden. Polynomdivision in \mathbb{E} liefert hier $\alpha^3 \equiv \alpha + 1 \pmod{u}$. Damit lässt sich nun die obige Rechnung fortsetzen:

$$\dots = 1 + \alpha^2 + \alpha + \alpha + 1 = \alpha^2.$$

(iv) Jetzt wird das Ergebnis mit π wieder zurück nach \mathbb{F}^n transformiert:

$$\pi(\alpha^2) = (0, 0, 1)^t.$$

(v) Im letzten Schritt kann nun die affine Abbildung T^{-1} angewendet werden:

$$\begin{aligned} T^{-1}((0, 0, 1)^t) &= M_T^{-1}((0, 0, 1)^t - v_T) = \\ &= \begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \left[\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} - \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \right] = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = m. \end{aligned}$$

Die Entschlüsselung hat also wie erwartet aus dem Geheimtext c die ursprüngliche Nachricht m rekonstruiert.

2.4 Sicherheitsbetrachtung von C^*

Obwohl die C^* -Chiffre eine elegante und interessante Umsetzung eines MQ -Kryptosystems darstellt, kann sie leider nicht mehr als sicher angesehen werden. Patarin analysierte das Verfahren in [Pat95] sehr detailliert. Es gelang ihm unter anderem ein allgemeiner Angriff auf C^* , der den Suchraum, also den Raum, in dem ein Angreifer zu einem Geheimtext nach passenden Klartexten suchen kann, so stark verkleinert, dass zu jedem Geheimtext stets der zugehörige Klartext gefunden werden kann. Dabei wird sogar ein bilinearer Zusammenhang zwischen Klartext und zugehörigem Geheimtext hergestellt. Das Verfahren arbeitet effizient, daher muss C^* als gebrochen betrachtet werden.

2.4.1 Einschränkung des Parameters λ

Der Parameter λ aus dem Exponenten der geheimen polynomiellen Abbildung P^* sollte bestimmten Anforderungen genügen, da anderenfalls unter Umständen Schwachstellen entstehen, die einen erfolgreichen Angriff ermöglichen können. Zum Verständnis folgt zunächst eine Definition.

Definition 2.4.1. Sei $\gamma \in \mathbb{Z}$. Dann bezeichnet $HW_k(\gamma)$ die Anzahl der von Null verschiedenen Elemente in der p -adischen Darstellung von γ zur Basis k . HW steht für „Hamming Weight“.

Bemerkung. Falls $k = 2$, so gibt $HW_2(\gamma)$ gerade die Anzahl der Einsen in der Binärdarstellung von γ an.

Eine Nachricht $x = (x_1, \dots, x_n)^t \in \mathbb{F}^n$ wird, wie bereits erläutert, zunächst durch T affin linear auf $a := Tx$ abgebildet und dann mit π^{-1} in den Erweiterungskörper \mathbb{E} , wieder aufgefasst als \mathbb{F} -Vektorraum zur Basis $\{\alpha_1, \dots, \alpha_n\}$, transformiert:

$$\mathbb{F}^n \xrightarrow{T} \mathbb{F}^n \xrightarrow{\pi^{-1}} \mathbb{E} : x = (x_1, \dots, x_n)^t \mapsto a = (a_1, \dots, a_n)^t \mapsto A = \sum_{i=1}^n a_i \alpha_i.$$

Jedes a_i , $i = 1, \dots, n$, kann entsprechend der affin linearen Abbildung $T : x \mapsto M_T x + v_T$ wie folgt geschrieben werden:

$$a_i = t_{i0} + \sum_{j=1}^n t_{ij} x_j,$$

wobei hier t_{ij} für $1 \leq i, j \leq n$ die Einträge in der Transformationsmatrix M_T und t_{i0} für $1 \leq i \leq n$ die Einträge des Vektors v_T sind.

Es ist nach Satz 2.2.2 bekannt, dass der Grundkörper \mathbb{F} die Charakteristik 2 hat, also $|\mathbb{F}| = 2^m$ für eine natürliche Zahl m . In der bisher verwendeten Notation hat eine Nachricht die Länge n , sie besteht also aus n Werten aus \mathbb{F} . Als Bitfolge in Binärdarstellung haben diese n Werte folglich insgesamt die Länge nm . Betrachtet man $a = (a_1, \dots, a_n) \in \mathbb{F}^n$, so kann man somit jeden Wert a_i , $i = 1, \dots, n$, als Bitfolge $a_{i1} \dots a_{im}$ schreiben. Zur Vermeidung der Doppelindeizes kann man nun a auch als reine Bitfolge $\bar{a}_1 \dots \bar{a}_{nm}$ schreiben. Im Folgenden deuten Variablen mit Überstrich solche reinen Bitfolgen an. Passt man in der affin linearen Abbildung T die Dimension von Matrix und Vektoren an die Länge nm der Bitfolge an, so erhält man entsprechend folgenden Zusammenhang für jedes \bar{a}_i , $i = 1, \dots, nm$:

$$\bar{a}_i = \bar{t}_{i0} + \sum_{j=1}^{nm} \bar{t}_{ij} \bar{x}_j.$$

Wie bereits in Satz 2.2.1 beschrieben, kann P^* und damit die Gleichung

$$X^{q^\lambda+1} = Y$$

in \mathbb{E} invertiert werden, und es gilt

$$X = Y^h, \quad h \in \mathbb{N}. \quad (2.7)$$

Sei a wie oben eine affin linear transformierte Nachricht x aus \mathbb{F}^n , und sei weiter $\pi^{-1}(a) = A \in \mathbb{E}$ die Transformation von a in den Erweiterungskörper und $P^*(A) = B$. Damit ist $A = B^h$. A bzw. a lässt sich also als Polynom in B bzw. b schreiben. Nun ist entscheidend, welchen Grad dieses Polynom über den Koeffizienten der Darstellung von a hat. Ist der Grad sehr klein, kann das System unter Umständen erfolgreich angegriffen werden.

Bemerkung. Der Grad kann in Abhängigkeit von der Darstellung von a variieren, wenn man $GF(2^m)$ als Vektorraum über verschiedenen Zwischenkörpern zwischen $GF(2^m)$ und $GF(2)$ betrachtet. Es lässt sich jedoch zeigen, dass der Grad in jeder Darstellung mit Koeffizienten aus $GF(2^l)$ für $l > 1$ mindestens so groß ist wie der Grad in der binären Darstellung über $GF(2)$. Insofern reicht es, diesen Fall als worst case Szenario abzuschätzen.

Die Darstellung mit binären Koeffizienten lässt sich realisieren, indem man $GF(2^m)$ als Körpererweiterung von $GF(2)$ betrachtet, sodass sich alle Elemente aus $GF(2^m)$ bei Wahl einer geeigneten Basis θ_i , $i = 1, \dots, m$ als Linearkombination mit Koeffizienten aus $GF(2)$ schreiben lassen. Es gilt dann ein einfacher Zusammenhang, der am folgenden Beispiel veranschaulicht wird: Sei $h = 13$, also $h = 1101$ in Binärschreibweise, und somit $HW_2(h) = 3$. Für $c \in GF(2^m)$ sind in dieser Darstellung die Koeffizienten \bar{c}_i , $i = 1, \dots, m$ in $GF(2)$ enthalten.

Da $|GF(2)| = 2$, gilt mit Frobenius und $\text{char}(GF(2^m)) = 2$:

$$\begin{aligned} c^h &= \left(\sum_{i=1}^m \bar{c}_i \theta_i \right)^{2^3+2^2+2^0} \\ &\stackrel{!}{=} \sum_{i=1}^m (\bar{c}_i)^{2^3} \theta_i^{2^3} \cdot \sum_{i=1}^m (\bar{c}_i)^{2^2} \theta_i^{2^2} \cdot \sum_{i=1}^m (\bar{c}_i)^{2^0} \theta_i^{2^0} \\ &\stackrel{!}{=} \sum_{i=1}^m \bar{c}_i \theta_i^{2^3} \cdot \sum_{i=1}^m \bar{c}_i \theta_i^{2^2} \cdot \sum_{i=1}^m \bar{c}_i \theta_i^{2^0}. \end{aligned}$$

Das Polynom hat also in den Koeffizienten den Grad $HW_2(h) = 3$. Identifiziert man $GF(2^m)$ mit dem Vektorraum $GF(2)^m$, lässt sich das Polynom also als ein System von Polynomen über den Koeffizienten auffassen. Wieder als reine Bitfolge betrachtet, kann somit \bar{a}_i , $i = 1, \dots, nm$, als Polynom vom Grad $HW_2(h)$ in den Unbekannten $\bar{b}_1 \dots \bar{b}_{nm}$ und damit $\bar{y}_1, \dots, \bar{y}_{nm}$ ausgedrückt werden, da b affin in y ist. Zusammengefasst ergibt sich nach (2.7) folgende Beziehung:

$$\bar{a}_i = \bar{t}_{i0} + \sum_{j=1}^{nm} \bar{t}_{ij} \bar{x}_j = p_i(\bar{y}_1, \dots, \bar{y}_{nm}), \quad i = 1, \dots, nm, \quad (2.8)$$

wobei hier p_i , $i = 1, \dots, nm$, für allgemeine Polynome vom Grad $HW_2(h)$ in den Unbekannten $\bar{y}_1 \dots \bar{y}_{nm}$ steht. Es gibt also mindestens nm Gleichungen vom Typ (2.8), die linear in \bar{x}_j sind und Grad $HW_2(h)$ über $\bar{y}_1 \dots \bar{y}_{nm}$ haben. Schreibt man nun die Polynome in allgemeiner Form mit den Koeffizienten als Unbekannten und setzt über die öffentliche Verschlüsselungsfunktion generierte Paare (x, y) in ausreichender Anzahl ein, so lassen sich mindestens nm linear unabhängige Gleichungen finden und man erhält ein lineares Gleichungssystem in den Koeffizienten der Polynome, mit dem sich der Lösungsraum der Koeffizienten bestimmen lässt. Zu gegebenem Geheimtext y lassen sich damit nun nm Gleichungen finden, die in den Bits \bar{x}_j des Klartextes linear sind, was die Entschlüsselung ermöglichen kann. Es ist klar, dass der Aufwand zur Bestimmung aller Koeffizienten der Polynome p_i von der Größe des Grades, also $HW_2(h)$, abhängt, da die Anzahl der Koeffizienten mit dem Grad der Polynome steigt. Daher ist dieser Angriff nur bei sehr kleinem Grad effizient durchführbar.

Es ist also wichtig, den Parameter λ für das C^* -System so zu wählen, dass $HW_2(h)$ nicht zu klein wird, damit die Erfolgsaussichten des beschriebenen Angriffs möglichst gering sind. Patarin empfiehlt dazu $HW_2(h) \geq 6$.

2.4.2 Patarins Angriff

In diesem Abschnitt wird nun der eigentliche Angriff von Patarin erläutert, der eine Entschlüsselung der C^* -Chiffre unabhängig von der Wahl der Parameter ermöglicht.

Patarins Angriff setzt direkt bei der geheimen Polynomabbildung

$$P^*(X) = X^{q^\lambda+1} = Y, \quad X, Y \in \mathbb{E} \quad (2.9)$$

über dem Erweiterungskörper \mathbb{E} an. Ziel des Angriffs ist es, X möglichst einfach aus Y bestimmen zu können. Wenn $HW_2(h)$ groß ist (vgl. vorigen Abschnitt),

bietet die Gleichung $X = Y^h$ keinen Angriffspunkt. Patarin konnte jedoch zeigen, dass die geheime Polynomabbildung durch relativ einfache Umformungen in eine Form überführt werden kann, in der sowohl X als auch Y linear vorliegen. Damit ist es dann möglich, ein bilineares Gleichungssystem in X und Y aufzustellen, mit dessen Hilfe ein Geheimtext entschlüsselt werden kann. Die Umformung erfolgt in zwei Schritten. Zunächst wird die Abbildung $g : x \mapsto x^{q^\lambda - 1}$ auf beide Seiten der Gleichung (2.9) angewendet:

$$X^{q^{2\lambda} - 1} = Y^{q^\lambda - 1}.$$

Dann wird die Gleichung mit XY multipliziert, und es ergibt sich

$$Y \cdot X^{q^{2\lambda}} = X \cdot Y^{q^\lambda}. \quad (2.10)$$

Die umgeformte Gleichung (2.10) weist einen entscheidenden Unterschied zur Ausgangsgleichung (2.9) auf: Sowohl X als auch Y kommen in (2.10) nur \mathbb{F} -linear vor, da sowohl $Y \mapsto Y^{q^\lambda}$ als auch $X \mapsto X^{q^{2\lambda}}$ \mathbb{F} -lineare Abbildungen sind, wie bereits in Abschnitt 2.2 erläutert. Es existiert nun also ein \mathbb{F} -linearer Zusammenhang zwischen X und Y , der es ermöglichen kann, X aus Y zu berechnen. Betrachtet man nun \mathbb{E} wieder als \mathbb{F} -Vektorraum, so ergeben sich n Gleichungen vom Typ (2.10) in den n unbekanntenen Koeffizienten der Darstellung von X als \mathbb{F} -Vektor. Es sind allerdings nicht alle n Gleichungen des entstehenden Systems notwendig linear unabhängig. Die Gleichungen lassen sich folgendermaßen schreiben:

$$\sum_{i=1}^n \sum_{j=1}^n \gamma_{ij} x_i y_j + \sum_{i=1}^n \mu_i x_i + \sum_{i=1}^n \nu_i y_i + \delta = 0. \quad (2.11)$$

Dabei sind x_i bzw. y_i , $i = 1, \dots, n$, aus \mathbb{F} die Koeffizienten von X bzw. Y in der Darstellung als \mathbb{F} -Vektoren. Setzt man hierfür Wertepaare ein, die man wieder über die öffentliche Polynom-Abbildung P bestimmt hat, so lässt sich (2.11) als Gleichung in $n^2 + n + n + 1 = (n+1)^2$ Unbekannten γ_{ij} , μ_i , ν_i , δ , $i, j = 1, \dots, n$, auffassen. Damit lässt sich ein Gleichungssystem aufstellen, mit dem die genannten Unbekannten ermittelt werden können. Dies ist der erste Teil des Angriffs. Er schafft als Ergebnis ein bilineares Gleichungssystem in den Koeffizienten x_i und y_i , $i = 1, \dots, n$, des Klar- bzw. Geheimtexts und damit die Grundlage für die Rekonstruktion von Klartexten. Dieses Gleichungssystem muss für ein C^* -System nur ein einziges Mal aufgestellt werden und kann dann zur Rekonstruktion beliebiger Klartexte verwendet werden. Der zweite Teil besteht darin, diese Komponenten (y_1, \dots, y_n) eines Geheimtexts y in das soeben erstellte Gleichungssystem einzusetzen, um dann die Komponenten (x_1, \dots, x_n) des Klartexts x zu bestimmen. Die Gleichungen müssen jedoch nicht unbedingt linear unabhängig sein. Daher ist im Allgemeinen nur eine Bestimmung von l Komponenten aus $\{x_1, \dots, x_n\}$ möglich, falls gerade l Gleichungen des Systems linear unabhängig sind. Für die Stärke des Angriffs ist also die Größe von l entscheidend. Patarin konnte jedoch folgende Abschätzung für l zeigen:

Satz 2.4.1. *Für die Anzahl l der linear unabhängigen Gleichungen vom Grad 1 in x_1, \dots, x_n in einem System vom Typ (2.11) gilt*

$$l \geq \frac{2n}{3}.$$

Beweis. Siehe [Pat95, S. 255ff]. □

Im Allgemeinen können also mindestens zwei Drittel der Komponenten eines beliebigen Klartexts rekonstruiert werden. Das heißt, dass durch Patarins Angriff die Dimension des Suchraums, also die Menge von Klartexten, in denen ein Angreifer den korrekten Klartext zu einem gegebenen Geheimtext vermuten kann, auf etwa ein Drittel der Größe von \mathbb{F}^n eingeschränkt werden kann. Ein Angreifer muss zu einem gegebenen Geheimtext auf der Suche nach dem zugehörigen Klartext nicht mehr ganz \mathbb{F}^n , sondern nur einen deutlich kleineren Teilraum durchsuchen. Dies kann effizient durchgeführt werden. Das C^* -Verfahren kann folglich nicht mehr als sicher angesehen werden. Patarins Angriff ist von besonders großer Bedeutung, da er das C^* -System unabhängig der gewählten Parameter brechen kann, da die entscheidende geheime Polynomabbildung, auf der die Funktionsweise des gesamten Systems beruht, in einen einfachen linearen Zusammenhang verwandelt werden konnte.

2.5 Fazit

Die C^* -Chiffre stellt mit der Implementierung eines MQ -Systems über gemischten Körpern einen eleganten Ansatz zur Verfügung, ein auf einem MQ -System basierendes Public Key Kryptosystem zu konstruieren. Da das System durch Patarin grundlegend gebrochen wurde, kann es allerdings nur noch als Ausgangspunkt für weitere Entwicklungen dienen. Der verhältnismäßig einfache und übersichtliche Aufbau des Systems lässt jedoch Spielraum für Modifikationen, so dass tatsächlich verschiedene modifizierte Systeme als Weiterentwicklungen der C^* -Chiffre entstanden sind. Einige dieser Modifikationen werden in den nächsten Kapiteln vorgestellt und analysiert.

Kapitel 3

Die Perturbed Matsumoto Imai Chiffre

3.1 Einleitung

Die C^* -Chiffre kann, wie im letzten Kapitel gezeigt, durch Patarins Angriff effizient gebrochen werden und daher nicht als sicher betrachtet werden. Dennoch stellt C^* einen interessanten Ausgangspunkt für die Umsetzung einer Public Key Chiffre auf Basis multivariater quadratischer Systeme dar. Es stellt sich die Frage, ob der vielversprechende Ansatz durch Modifikationen so erweitert werden kann, dass unter Beibehaltung des grundsätzlichen Konzepts eine neue Public Key Chiffre entstehen kann, die höhere Sicherheit bietet und den bekannten Angriffen standhält. Es gibt verschiedene Ansätze für derartige Modifikationen, ein interessanter Kandidat ist die Perturbed Matsumoto Imai Chiffre (vgl. [Din04]). Bei dieser Variante wird das zugrunde liegende MQ -System der C^* -Chiffre durch zeilenweise Addition zusätzlicher quadratischer Polynome gestört (engl. „perturbed“). Diese Polynome werden zufällig gewählt. Das Perturbed Matsumoto Imai System widersteht Patarins Angriff und erreicht somit ein höheres Sicherheitsniveau als das zugrunde liegende C^* -System. Im nächsten Abschnitt wird die Funktionsweise der Perturbed Matsumoto Imai Chiffre näher erläutert.

3.2 Funktionsweise

Ziel bei der Entwicklung der Perturbed Matsumoto Imai Chiffre war es, eine Modifikation zu konstruieren, die dem Linearisierungsangriff von Patarin widersteht, ohne die Effizienz des Systems zu sehr zu beeinträchtigen. Die Idee, zu diesem Zweck das MQ -System mit zusätzlichen Polynom-Termen zu modifizieren, wurde bereits bei anderen Varianten der C^* -Chiffre verwendet, beispielsweise bei der „Oil and Vinegar“ Methode. Das Konzept bei der Perturbed Matsumoto Imai Chiffre weicht jedoch davon ab, da es, statt zusätzliche „externe“ Variablen für die Modifikation zu verwenden, auf die bereits vorhandenen „internen“ Variablen zurückgreift, um die Störung zu modellieren. Das heißt, dass die vorhandenen Zeilen des MQ -Systems gestört werden und nicht etwa das System um weitere Variablen oder Zeilen erweitert wird. Die Störung wird dabei mög-

lichst klein gehalten, um die Effizienz des Systems nicht zu sehr zu beeinflussen. Konkret heißt das, dass die Variable r im Folgenden klein gewählt wird.

3.2.1 Die Gestalt der Störung

Das Störungspolynom

Zur Konstruktion der Perturbed Matsumoto Imai Chiffre wird zunächst ein System von r linear unabhängigen affin linearen Abbildungen über \mathbb{F}^n definiert:

$$z_i = \sum_{j=1}^n \alpha_{ij} x_j + \beta_i, \quad i = 1, \dots, r \quad (3.1)$$

Die Koeffizienten α_{ij} und β_i aus \mathbb{F} , für $i = 1, \dots, r$ und $j = 1, \dots, n$, werden dabei zufällig gewählt. Mit Hilfe der z_i , $i = 1, \dots, r$, lässt sich nun folgende surjektive affin lineare Abbildung konstruieren:

$$Z : \mathbb{F}^n \rightarrow \mathbb{F}^r : (x_1, \dots, x_n) \mapsto (z_1, \dots, z_r) \quad (3.2)$$

Als nächstes wird nun die innere polynomielle Abbildung $\tilde{P} : \mathbb{F}^n \rightarrow \mathbb{F}^n$, also das unverschleierte MQ -System aus der C^* -Chiffre, modifiziert, indem zufällig gewählte quadratische Polynome p_j , $j = 1, \dots, n$, in den r Variablen z_i , $i = 1, \dots, r$, addiert werden. Das entstehende neue MQ -System sei als $\bar{\bar{P}}$ bezeichnet. Es gilt also

$$\begin{aligned} \bar{\bar{P}}(x_1, \dots, x_n) &= (\bar{\bar{P}}_1(x_1, \dots, x_n), \dots, \bar{\bar{P}}_n(x_1, \dots, x_n)) \\ &:= (\tilde{P}_1(x_1, \dots, x_n) + p_1(z_1, \dots, z_r), \dots, \tilde{P}_n(x_1, \dots, x_n) + p_n(z_1, \dots, z_r)) \end{aligned}$$

Die Polynome p_j , $j = 1, \dots, n$, sind quadratisch und als MQ -System somit nicht effizient lösbar. Dies ist notwendig, damit bei Kenntnis eines Bildwertes dieses Polynomsystems keine effiziente Berechnung des Urbildes möglich ist, denn sonst ließe sich auf diesem Wege möglicherweise der Klartext rekonstruieren. Die Polynome lassen sich durch Vektorschreibweise zu einer polynomiellen Abbildung

$$p(z_1, \dots, z_r) = (p_1(z_1, \dots, z_r), \dots, p_n(z_1, \dots, z_r))$$

von \mathbb{F}^r nach \mathbb{F}^n zusammenfassen. Durch Komposition mit Z lässt sich diese Abbildung sogar über \mathbb{F}^n darstellen:

Definition 3.2.1. Es seien p, Z wie oben gewählt. Dann wird \tilde{p} mit

$$\tilde{p} : \mathbb{F}^n \rightarrow \mathbb{F}^n : (x_1, \dots, x_n) \mapsto (p \circ Z)(x_1, \dots, x_n)$$

als das *Störungspolynom* bezeichnet.

Die gestörte Verschlüsselungsabbildung

Zusammengefasst lässt sich die innere polynomielle Abbildung der Perturbed Matsumoto Imai Chiffre also wie folgt schreiben:

$$\bar{\bar{P}} = \tilde{P} + \tilde{p} \quad (3.3)$$

Damit lässt sich die öffentliche polynomielle Abbildung der Perturbed Matsumoto Imai Chiffre folgendermaßen definieren:

$$\widehat{P}(x_1, \dots, x_n) := (S \circ \bar{P} \circ T)(x_1, \dots, x_n) \quad (3.4)$$

Die Verschlüsselungsabbildung \widehat{P} der Perturbed Matsumoto Imai Chiffre weist also die klassische Gestalt einer auf MQ -Systemen basierenden Public Key Chiffre auf. Nur das zugrunde liegende MQ -System ist im Vergleich zur C^* -Chiffre modifiziert. Da das Störungspolynom zufällig gewählt wird, ist das innere MQ -System der Perturbed Matsumoto Imai Chiffre im Gegensatz zu dem der C^* -Chiffre nun von ganz allgemeiner Form. Die Verschlüsselungsfunktion ist daher nicht mehr bijektiv. Es können also mehrere Klartexte zum selben Geheimtext führen. Bei der Entschlüsselung muss daher gegebenenfalls noch der richtige Klartext identifiziert werden. Dieser Umstand wird später noch näher erläutert.

Die Störungsmenge

Um die Perturbed Matsumoto Imai Chiffre verwenden zu können, muss die „Störung“ durch das neu addierte Polynomsystem \tilde{p} bei der Entschlüsselung wieder rückgängig gemacht werden können. Dazu muss zuerst dieses Störungspolynom, genauer dessen Wert, entfernt werden, so dass anschließend ein herkömmliches C^* -System vorliegt, dessen innere polynomielle Abbildung \widehat{P} wie gehabt invertiert werden kann. Das Problem ist nun, dass bei der Entschlüsselung eines Geheimtexts die zu entfernenden Störungsterme (zeilenweise betrachtet) im Bildbereich des Störungspolynoms \tilde{p} liegen und zu diesem Zeitpunkt weder das Bild noch das Urbild des Störungspolynoms bekannt ist. Denn es ist nur das Bild der Verschlüsselungsabbildung \widehat{P} , der Geheimtext, bekannt, nicht aber das Bild von \tilde{p} und auch nicht das Urbild, der Klartext, aus dem sich das Bild des Störungspolynoms, die Störungsterme, berechnen ließe. Es ist also unklar, welcher Wert subtrahiert werden muss, um die Störung zu entfernen. Beim Entschlüsselungsvorgang muss genau das Bildelement des Störungspolynoms entfernt werden, das zum verschlüsselten Klartext, genauer zu $T(x_1, \dots, x_n)$, gehört. Der Klartext (x_1, \dots, x_n) ist aber zu diesem Zeitpunkt noch nicht bekannt, somit ist auch nicht klar, welches das korrekte Bildelement ist, da dieses aus dem Geheimtext nicht zu ersehen ist. Es reicht also bei der Entschlüsselung nicht aus, das Störungspolynom allein zu kennen. Es müssen passende Urbild/Bild-Paare vorliegen, die allerdings natürlich mit Hilfe des Störungspolynoms berechnet werden können. Das Problem wird im Abschnitt 3.4 noch näher erläutert.

Zur Lösung des Problems wird daher die Menge M_p definiert, die Tupel mit zwei Komponenten enthält. Die erste Komponente ist ein Bildelement des Störungspolynoms, die zweite ist die Menge der zu diesem Bildelement gehörenden Urbildelemente. Es wird hierbei allerdings die Abbildung p betrachtet, die ja ein Bestandteil des Störungspolynoms \tilde{p} ist. Genauer:

Definition 3.2.2. Sei $\tilde{p} = (p \circ Z)$ das Störungspolynom wie oben beschrieben und sei $\text{im}(p) = \text{im}(\tilde{p})$ das Bild der Abbildung p . Dann bezeichnet

$$M_p := \{(\lambda, \mu) : \lambda \in \text{im}(p), \mu = \{(z_1, \dots, z_r) : p(z_1, \dots, z_r) = \lambda\}\}$$

die *Störungsmenge*.

Bemerkung. Der Urbildraum des Störungspolynoms p ist \mathbb{F}^r , es kann also nur $|\mathbb{F}^r| = q^r$ verschiedene Urbilder geben. Die Anzahl der Elemente der Störungsmenge M_p kann somit höchstens q^r sein. Wegen $r \ll n$ sind der Raum \mathbb{F}^r und damit auch die Störungsmenge deutlich kleiner als der Klartextrraum \mathbb{F}^n . Andernfalls wäre der Aufwand, die Störungsmenge nach einem korrekten Tupel für die Entschlüsselung zu durchsuchen, zu groß.

Im Folgenden wird nun der Ablauf der Ver- und Entschlüsselung mit der Perturbed Matsumoto Imai Chiffre näher betrachtet.

3.3 Verschlüsselung

Der Ablauf der Verschlüsselung bei der Perturbed Matsumoto Imai Chiffre ist nahezu identisch mit dem der C^* -Chiffre. Der öffentliche Schlüssel ist zwar modifiziert, allerdings ist diese Tatsache für den Nutzer des öffentlichen Schlüssels nicht transparent, die Modifikation ändert den Ablauf also nicht.

3.3.1 Öffentlicher Schlüssel

Der öffentliche Schlüssel besteht aus folgenden Elementen:

1. Dem Grundkörper \mathbb{F} mit zugehöriger Multiplikation und Addition sowie der Länge n der Nachrichten
2. Der polynomiellen Abbildung \hat{P}

3.3.2 Ablauf der Verschlüsselung

Eine Nachricht $(x_1, \dots, x_n) \in \mathbb{F}^n$ wird verschlüsselt, indem $\hat{P}(x_1, \dots, x_n)$ berechnet wird, das Ergebnis ist der Geheimtext $(y_1, \dots, y_n) \in \mathbb{F}^n$. Um die Übersicht über den Ablauf der Entschlüsselung im nächsten Abschnitt in Hinblick auf die Bezeichnungen zu erleichtern, werden die einzelnen Schritte der Verschlüsselung nun kurz beschrieben.

- (i) Auf den Klartext $m = (x_1, \dots, x_n)$ wird die affin lineare Abbildung T angewendet:

$$T(x_1, \dots, x_n) =: (y'_1, \dots, y'_n).$$

- (ii) Die Anwendung von \bar{P} ergibt dann:

$$\begin{aligned} \bar{P}(y'_1, \dots, y'_n) &= (\tilde{P} + \tilde{p})(y'_1, \dots, y'_n) \\ &= \tilde{P}(y'_1, \dots, y'_n) + \tilde{p}(y'_1, \dots, y'_n) \\ &= \tilde{P}(y'_1, \dots, y'_n) + (p \circ Z)(y'_1, \dots, y'_n) \\ &= \tilde{P}(y'_1, \dots, y'_n) + \underbrace{p(z'_1, \dots, z'_r)}_{\in \mu} \\ &=: (y''_1, \dots, y''_n). \end{aligned}$$

- (iii) Im letzten Schritt wird nun S angewendet und damit der Geheimtext c berechnet:

$$S(y''_1, \dots, y''_n) = (y_1, \dots, y_n) = c.$$

3.4 Entschlüsselung

Im Gegensatz zur Verschlüsselung beeinflusst die Modifikation des Systems den Ablauf beim Entschlüsseln deutlich. Zunächst wird die Störung rückgängig gemacht, so dass ein unverändertes C^* -System vorliegt. Dieses kann dann nach der herkömmlichen Methode entschlüsselt werden. Der private Schlüssel umfasst dazu verglichen mit C^* einige zusätzliche Komponenten.

3.4.1 Privater Schlüssel

Die Komponenten des privaten Schlüssels sind:

1. Die polynomielle Abbildung P^* des zugrunde liegenden C^* -Systems
2. Die beiden affin linearen Abbildungen S und T
3. Die Abbildung Z
4. Die Störungsmenge M_p bzw. das Polynom p

3.4.2 Ablauf der Entschlüsselung

Bei der Entschlüsselung wird in mehreren Schritten vorgegangen. Für Details bezüglich der C^* betreffenden Schritte sei auf Kapitel 2 verwiesen. In diesem Abschnitt werden hauptsächlich die durch die Modifikation hinzugekommenen Neuerungen betrachtet.

- (i) Der Geheimtext sei

$$\begin{aligned} c = (y_1, \dots, y_n) &= \widehat{P}(x_1, \dots, x_n) \\ &= (S \circ \bar{P} \circ T)(x_1, \dots, x_n) \\ &= (S \circ (\tilde{P} + \tilde{p}) \circ T)(x_1, \dots, x_n). \end{aligned}$$

Es muss als erstes die Abbildung S^{-1} angewendet werden, um S rückgängig zu machen. Es wird also

$$S^{-1}(y_1, \dots, y_n) = (y_1'', \dots, y_n'')$$

berechnet.

- (ii) Im nächsten Schritt soll nun $\tilde{p}(y_1', \dots, y_n')$, genauer $\tilde{p}(T(x_1, \dots, x_n))$, entfernt werden, damit die unmodifizierte C^* -Struktur zurückbleibt, deren Entschlüsselung dann gemäß der üblichen Methode erfolgen kann. Um diesen addierten Störungsterm wieder zu subtrahieren, muss er explizit bekannt sein. Da aber der Klartext (x_1, \dots, x_n) zu diesem Zeitpunkt noch nicht bekannt ist, ist auch $\tilde{p}(T(x_1, \dots, x_n))$ unbekannt. Es wird daher nun die Menge M_p herangezogen, mit deren Hilfe alle in Frage kommenden Werte λ des Störungsterms überprüft werden können. Da der korrekte Wert λ somit nur heuristisch ermittelt werden kann, entspricht dieses Vorgehen einer erschöpfenden Suche in M_p und ist entsprechend aufwendig in

Hinblick auf die Effizienz des Verfahrens. Es wird nun ein Wert λ' aus M_p gewählt und vom bisherigen Ergebnis (y''_1, \dots, y''_n) subtrahiert:

$$(y''_1, \dots, y''_n) - \lambda' \stackrel{?}{=} \tilde{P}(y'_1, \dots, y'_n).$$

Die Gleichheit gilt, wenn λ' der korrekte Wert λ war.

Bemerkung. Wird als Grundkörper $\mathbb{F} = GF(2)$ mit der XOR-Verknüpfung als Addition verwendet, sind Addition und Subtraktion identisch. Es wird daher oft in obiger Schreibweise ein „+“ statt eines „-“ verwendet.

- (iii) Nachdem nun die Störung rückgängig gemacht ist, liegt ein klassisches C^* -System vor. Die Abbildung \tilde{P} kann nun also über dem Erweiterungskörper \mathbb{E} invertiert werden. Dabei ist zu beachten, dass die Korrektheit aller folgenden Werte noch davon abhängt, ob das korrekte λ gewählt wurde. Dies wird erst im nachfolgenden Schritt verifiziert. Bis dahin wird diese Abhängigkeit durch eine Indexierung mit λ' deutlich gemacht.

$$(y'_{\lambda'_1}, \dots, y'_{\lambda'_n}) = (\pi \circ (P^*)^{-1} \circ \pi^{-1})((y''_1, \dots, y''_n) - \lambda')$$

- (iv) Nun kann überprüft werden, ob das zuvor gewählte λ' korrekt war oder nicht. War es korrekt, dann muss es das Bild des im letzten Schritt berechneten Urbilds unter der Abbildung $\tilde{p} = p \circ Z$ sein. Dazu wird

$$Z(y'_{\lambda'_1}, \dots, y'_{\lambda'_n}) \stackrel{?}{\in} \mu'$$

überprüft, wobei μ' das zu dem oben gewählten λ' korrespondierende Element des Tupels aus M_p ist. Fällt diese Überprüfung positiv aus, dann ist $\lambda' = \lambda$ und $\mu' = \mu$ und es kann mit dem nächsten Schritt fortgefahren werden. Fällt sie hingegen negativ aus, wurde ein falscher Wert λ' gewählt und das erhaltene Ergebnis $(y'_{\lambda'_1}, \dots, y'_{\lambda'_n})$ wird ignoriert. In jedem Fall werden alle Tupel $(\lambda', \mu') \in M_p$ auf diese Weise beginnend bei Schritt (ii) überprüft, da es möglich ist, dass mehrere Tupel positiv geprüft werden. Das liegt daran, dass das MQ -System des Perturbed Matsumoto Imai Systems im Gegensatz zu C^* nicht mehr von spezieller Gestalt, sondern aufgrund des zufällig gewählten Störpolynoms von allgemeiner Form ist (vgl. Definition 1.2.1). Damit ist das System nicht mehr bijektiv wie bei C^* , ein Geheimtext kann also unter Umständen mehrere mögliche Klartexte besitzen, nämlich bis zu $|M_p| \leq q^r$ viele. Dies äußert sich dann in einer entsprechend größeren Anzahl von positiven Überprüfungen der Tupel aus M_p .

- (v) Im letzten Schritt wird nun die Abbildung T umgekehrt und somit der Klartext berechnet.

$$T^{-1}(y'_{\lambda'_1}, \dots, y'_{\lambda'_n}) = (x_{\lambda'_1}, \dots, x_{\lambda'_n})$$

Falls sich im vorigen Schritt (iv) genau ein Wert für $(y'_{\lambda'_1}, \dots, y'_{\lambda'_n})$ ergeben hat, so ist das nun im letzten Schritt erhaltene Ergebnis der Klartext. Sollten es jedoch mehrere Werte sein, da es mehrere positive Überprüfungen für Tupel aus M_p gab, so muss eine Technik verwendet werden, um den Klartext eindeutig identifizieren zu können. Ein mögliche Methode hierfür

ist beispielsweise die Verwendung von Hash-Werten, mit deren Hilfe der richtige Klartext ermittelt werden kann. Dazu wird vor der Verschlüsselung einer Nachricht der Hashwert des Klartextes berechnet und als Prüfsumme an den Klartext angehängt. Dann wird die komplette Zeichenfolge verschlüsselt. Nach der Entschlüsselung wird die Prüfsumme wieder von der Zeichenfolge separiert, und es wird durch Berechnung des Hashwertes überprüft, ob die Prüfsumme zum vermuteten Klartext gehört. Dies ist nur beim korrekten Klartext der Fall, der somit identifiziert werden kann. Tatsächlich ist dieses Problem in der Praxis aber relativ klein, da derartige Vielfachheiten nur selten auftreten, wie Computerexperimente gezeigt haben (siehe [Din04]).

3.5 Empfohlene Parameter

Ding schlägt in [Din04] die Implementierung eines Perturbed Matsumoto Imai Systems über $\mathbb{F} = GF(2)$ mit den Parametern $q = 2$, $n \geq 96$, $\lambda \geq 40$ sowie $r \geq 5$ vor, um einen Sicherheitslevel von 2^{80} zu erreichen.

3.6 Einfluss der Störung auf die Effizienz des Systems

Betrachtet man den Einfluss der Modifikation in der Perturbed Matsumoto Imai Chiffre auf die Effizienz des Verfahrens im Vergleich mit der C^* -Chiffre, so wird deutlich, dass der Aufwand der Entschlüsselung wahrnehmbar gestiegen ist, während die Verschlüsselung nur geringfügig beeinträchtigt wird. Der Einfluss auf die Effizienz der Entschlüsselung resultiert hauptsächlich aus der Tatsache, dass im Allgemeinen eine erschöpfende Suche über der Störungsmenge M_p durchgeführt werden muss, um die korrekten Tupel (λ, μ) zu finden. Daher ist die Größe dieser Menge entscheidend für die Höhe der Effizienzeinbuße. Wie schon oben beschrieben, gilt für die Mächtigkeit $|M_p| \leq q^r$, wobei q die Anzahl der Elemente des Grundkörpers \mathbb{F} ist, und r die Anzahl der affin linearen Abbildungen z_i bzw. die Dimension des Bildraums der Abbildung Z ist. Der Parameter r wird aber bewußt klein gewählt und als Grundkörper ist die Wahl eines kleinen Körpers wie beispielsweise $GF(2)$ möglich, so dass die Beeinträchtigung der Effizienz der Entschlüsselung durch die Modifikation um den Faktor q^r also angesichts einer Erhöhung der Sicherheit des Verfahrens als tolerierbar angesehen werden kann.

3.7 Fazit

Offenbar ist die Perturbed Matsumoto Imai Chiffre gegen Patarins Angriff resistent. Der Angriff setzt bei der polynomiellen Abbildung über dem Erweiterungskörper ein Monom von C^* -Gestalt voraus, bei der Perturbed Matsumoto Imai Chiffre ist dies aber aufgrund des addierten Störungspolynoms nicht mehr der Fall. Damit scheint der entscheidende Schwachpunkt der C^* -Chiffre beseitigt zu sein. Doch leider haben genauere Analysen der Perturbed Matsumoto

Imai Chiffre zeigt, dass es eine Möglichkeit gibt, die Störung des Systems nahezu unwirksam zu machen. Das System wird dabei zumindest soweit entstört, dass es bei nur geringem Mehraufwand wieder durch die Attacke von Patarin gebrochen werden kann. Dieser neue Angriff auf die Perturbed Matsumoto Imai Chiffre wird im folgenden Abschnitt analysiert.

Kapitel 4

Ein differentieller Angriff auf die Perturbed Matsumoto Imai Chiffre

4.1 Einleitung

Auf den ersten Blick scheint die Perturbed Matsumoto Imai Chiffre resistent gegen Patarins Angriff zu sein, da dieser sich auf das komplexere Polynom des Perturbed Matsumoto Imai Systems nicht anwenden lässt. Fouque, Granboulan und Stern haben jedoch in [FGS05] Schwächen dieses Systems aufgedeckt, die einen Angriff ermöglichen. Indem sie eine Methode fanden, den Klartextrraum in spezielle affine Teilräume zu zerlegen, konnten sie Bedingungen schaffen, unter denen die Störung des Systems weitestgehend unwirksam wird. Als Folge lässt sich dann mit Hilfe von Patarins Angriff wie bei C^* ein bilinearer Zusammenhang zwischen Klartext und Geheimtext herstellen, so dass bei gegebenem Geheimtext der passende Klartext leicht berechnet werden kann. Zunächst wird nun die Idee erläutert, die die Grundlage dieses Angriffs darstellt.

4.2 Idee und Motivation

Die höhere Sicherheit der Perturbed Matsumoto Imai Chiffre im Vergleich zur C^* -Chiffre wird durch die Addition des Störungspolynoms erreicht. Der Wert dieses Störungspolynoms ist dabei vom verschlüsselten Klartext abhängig und ist somit im Allgemeinen für verschiedene Klartexte unterschiedlich. Es erscheint daher schwierig, diese Störung rückgängig zu machen. Eine nähere Betrachtung des Störungsterms zeigt aber, dass die Störung für bestimmte Klassen von Klartexten gleich ist. Dies ist der entscheidende Punkt für den Angriff. Bei Kenntnis dieser Klassen kann die Störung somit klassenweise als konstant betrachtet werden. Obwohl dieser konstante Störungsterm das System noch vom klassischen C^* -System unterscheidet, lässt sich Patarins Angriff nun aber mit bestimmten Einschränkungen anwenden. Diese Erkenntnis liefert die Motivation, nach derartigen Klassen von Klartexten zu suchen. Zunächst wird nun aber erläutert, wie Patarins Angriff bei einer konstanten Störung angewendet werden kann.

4.2.1 Patarins Angriff bei konstanter Störung

Zur Erinnerung: Bei Patarins Angriff auf das C^* -System wird die geheime polynomielle Abbildung

$$X^{q^\lambda+1} = Y, \quad X, Y \in \mathbb{E},$$

überführt in den bilinearen Zusammenhang

$$Y \cdot X^{q^{2\lambda}} = X \cdot Y^{q^\lambda}$$

über \mathbb{E} , der sich über \mathbb{F}^n als bilineares Gleichungssystem der Form

$$\sum_{i=1}^n \sum_{j=1}^n \gamma_{ij} x_i y_j + \sum_{i=1}^n \mu_i x_i + \sum_{i=1}^n \nu_i y_i + \delta = 0$$

schreiben lässt. Für nähere Details zur Funktionsweise des Angriffs von Patarin sei auf Abschnitt 2.4.2 verwiesen. Es soll nun die Situation beim Übergang zum Perturbed Matsumoto Imai System betrachtet werden unter der Voraussetzung der Kenntnis einer Unterteilung des Klartextraums \mathbb{F}^n in Klassen, so dass jeweils alle Klartexte einer Klasse die gleiche Störung verursachen. Details zur Gestalt dieser Klassen werden später behandelt. Die verschiedenen Klassen seien mit

$$K_j, \quad j \in \mathbb{N},$$

bezeichnet. Um eine konstante Störung zu betrachten, werden nun also nur die Klartext/Geheimtext-Paare betrachtet, deren Klartexte in derselben Klasse liegen. Diese Klasse sei hier zur Veranschaulichung als K bezeichnet. Innerhalb der Klasse K ist die Störung also konstant und unabhängig vom Klartext. Sei $h \in \mathbb{F}^n$ der Wert dieser von den Klartexten aus K verursachten Störung, dann lässt sich die Situation für das innere MQ -System folgendermaßen darstellen:

$$\bar{P}(x) = \tilde{P}(x) + \tilde{p}(x) = \tilde{P}(x) + h = y', \quad x \in K \subseteq \mathbb{F}^n, \quad y', h \in \mathbb{F}^n$$

(Dabei wurden die gleichen Variablen x, y wie oben verwendet, y' zeigt an, dass der Geheimtext durch die Störung vom Geheimtext des C^* -Systems abweicht.) Betrachtet man nun wieder die in den Erweiterungskörper \mathbb{E} transferierte Abbildung, so ergibt sich für die geheime polynomielle Abbildung folgender Zusammenhang:

$$X^{q^\lambda+1} = Y' - H, \quad X \in \pi^{-1}(K) \subseteq \mathbb{E}, \quad Y', H \in \mathbb{E}$$

wobei $\pi^{-1}(K)$ wie gehabt die nach \mathbb{E} transformierte Menge $K \subseteq \mathbb{F}^n$ ist. Die Umformung von Patarin ergibt dann

$$(Y' - H) \cdot X^{q^{2\lambda}} = X \cdot (Y' - H)^{q^\lambda}.$$

Im letzten Schritt ergibt dies dann wieder einen bilinearen Zusammenhang

$$\sum_{i=1}^n \sum_{j=1}^n \gamma'_{ij} x_i y'_j + \sum_{i=1}^n \mu'_i x_i + \sum_{i=1}^n \nu'_i y'_i + \delta' = 0, \quad (4.1)$$

wobei $x_i, y'_i, i = 1, \dots, n$, die Komponenten des Klartexts $x \in K \subseteq \mathbb{F}^n$ bzw. des zugehörigen Geheimtexts $y' \in \mathbb{F}^n$ sind. Um die Koeffizienten $\gamma'_{ij}, \mu'_i, \nu'_i$

und $\delta', i, j = 1, \dots, n$, zu bestimmen, in die nun auch die konstante Störung h eingegangen ist, müssen bei Patarins Angriff mehrere Klartext/Geheimtext-Paare verwendet werden, um mit ihrer Hilfe ein Gleichungssystem in den Koeffizienten aufzustellen. Genau dieser Schritt ist beim Perturbed Matsumoto Imai System nur möglich, wenn die Störung für alle diese Klartext/Geheimtext-Paare identisch ist, da ansonsten die Koeffizienten bei jeder neuen Gleichung (4.1) durch die aus dem neuen Klartext resultierende neue Störung verändert würden, da sie von der Störung beeinflusst werden. Somit ist klar, dass Patarins Angriff auf das Perturbed Matsumoto Imai System nur funktionieren kann, wenn es Klassen von Klartexten gibt, die die gleiche Störung verursachen, so dass genügend Gleichungen für die Erstellung eines Gleichungssystems aufgestellt werden können. Ein solches Gleichungssystem ist dann allerdings nur für die Klartext/Geheimtext-Paare gültig, deren Klartexte aus der entsprechenden Klasse stammen. Um den ganzen Klartextrraum \mathbb{F}^n abzudecken, ist also eine Unterteilung des Raums in mehrere solcher Klassen nötig, so dass zu jeder Klasse ein eigenes Gleichungssystem aufgestellt werden kann. Erst dann ist wirklich für alle Klartext/Geheimtext-Paare aus \mathbb{F}^n ein bilinearer Zusammenhang gegeben. Mit den Überlegungen dieses Abschnitts ist nun die motivierende Grundlage für die Suche nach derartigen Klassen von Klartexten gegeben.

4.2.2 Klartextklassen mit konstanter Störung

Zunächst werden die den Störungsterm betreffenden relevanten Begriffe und Bezeichnungen wiederholt. Sei $(x'_1, \dots, x'_n) := T(x_1, \dots, x_n)$. Die Perturbed Matsumoto Imai Chiffre verwendet als Störungsterm ein zusätzlich addiertes quadratisches Polynom $\tilde{p} : \mathbb{F}^n \rightarrow \mathbb{F}^n$ der folgenden Form (vgl. Abschnitt 3.2):

$$\tilde{p}(x'_1, \dots, x'_n) = (p \circ Z)(x'_1, \dots, x'_n) = p(z_1, \dots, z_r),$$

wobei die affin lineare Abbildung Z folgendermaßen definiert ist:

$$Z : \mathbb{F}^n \rightarrow \mathbb{F}^r : (x'_1, \dots, x'_n) \mapsto (z_1, \dots, z_r)$$

mit

$$z_i = \sum_{j=1}^n \alpha_{ij} x'_j + \beta_i, \quad i = 1, \dots, r, \quad \text{und } \alpha_{ij}, \beta_i \in \mathbb{F},$$

$p : \mathbb{F}^r \rightarrow \mathbb{F}^n$ ist ein quadratisches Polynom.

Für den Angriff ist es nun erforderlich, dass der Wert dieses Störungspolynoms innerhalb bestimmter Klassen von Klartexten gleich bleibt. Dies ist der Fall, wenn der Eingabevektor (z_1, \dots, z_r) des Polynoms p unabhängig von diesen Klartexten ist. Genau das wird erreicht, wenn als Klasse die Klartexte betrachtet werden, die im Kern des linearen Teils der affin linearen Abbildung $Z \circ T$ liegen. Dies wird nun näher erläutert.

Der Raum \mathcal{K}

Die Komposition zweier affin linearer Abbildungen ist wieder affin linear, somit ist $Z \circ T : \mathbb{F}^n \rightarrow \mathbb{F}^r$ eine affin lineare Abbildung. Diese wird nun zunächst zur besseren Handhabung vereinfacht dargestellt. Das Bild von $Z \circ T$ lässt sich für einen Klartext $x = (x_1, \dots, x_n)^t \in \mathbb{F}^n$ folgendermaßen schreiben:

$$\begin{aligned} (Z \circ T)(x) &=: \begin{pmatrix} \sum_{j=1}^n \alpha'_{1j} x_j + \beta'_1 \\ \vdots \\ \sum_{j=1}^n \alpha'_{rj} x_j + \beta'_r \end{pmatrix} \\ &= \begin{pmatrix} \alpha'_{11} & \cdots & \alpha'_{1n} \\ \vdots & & \vdots \\ \alpha'_{r1} & \cdots & \alpha'_{rn} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} \beta'_1 \\ \vdots \\ \beta'_r \end{pmatrix} \\ &=: Ax + \beta', \end{aligned} \tag{4.2}$$

wobei A die $(r \times n)$ -Matrix der Koeffizienten ist, die den linearen Teil der Abbildung $Z \circ T$ beschreibt. β' ist entsprechend ein Vektor aus \mathbb{F}^r .

Definition 4.2.1. Seien die affin lineare Abbildung $Z \circ T$ sowie die Matrix A wie oben definiert. Für $x = (x_1, \dots, x_n)^t \in \mathbb{F}^n$ sei

$$\begin{aligned} (Z \circ T)_l(x) &:= \left(\sum_{j=1}^n \alpha'_{1j} x_j, \dots, \sum_{j=1}^n \alpha'_{rj} x_j \right)^t \\ &= Ax \end{aligned}$$

als der *lineare Teil* der Abbildung $Z \circ T$ bezeichnet. Dann ist

$$\mathcal{K} := \ker(Z \circ T)_l = \{x \in \mathbb{F}^n : (Z \circ T)_l(x) = 0\}$$

der Kern des linearen Teils der Abbildung $Z \circ T$.

Bemerkung. \mathcal{K} ist also der Lösungsraum des homogenen linearen Gleichungssystems $Ax = 0$ und ein Untervektorraum von \mathbb{F}^n .

Es soll nun untersucht werden, welche Störung die Klartexte aus \mathcal{K} verursachen. Für jeden Klartext $x = (x_1, \dots, x_n)^t \in \mathcal{K}$ gilt

$$\begin{aligned} (Z \circ T)(x) &= \underbrace{Ax}_{=0} + \beta' \\ &= \beta' \\ &= (\beta'_1, \dots, \beta'_r)^t, \end{aligned}$$

die Störung ist somit für alle diese $x \in \mathcal{K}$ identisch, nämlich $p(\beta'_1, \dots, \beta'_r)$. Der Raum \mathcal{K} stellt also tatsächlich eine Klasse mit der gewünschten Eigenschaft dar. Es gibt aber darüber hinaus weitere Klassen von Klartexten, deren resultierende Störung ebenfalls innerhalb der Klasse konstant ist. Es sind die Nebenklassen von \mathcal{K} .

Die Nebenklassen von \mathcal{K}

Die Nebenklassen haben folgende Gestalt:

Definition 4.2.2. Sei $\mathcal{K} \subseteq \mathbb{F}^n$ wie oben definiert. Dann bezeichnet

$$K_j := \kappa_j + \mathcal{K}, \quad \kappa_j \in \mathbb{F}^n, j \in \mathbb{N},$$

die Nebenklassen von \mathcal{K} . Festlegung: $K_0 := \mathcal{K}$.

Bemerkung. Aus der Linearen Algebra ist bekannt, dass $\mathcal{K} \subseteq \mathbb{F}^n$ ein Untervektorraum von \mathbb{F}^n ist. Jede Nebenklasse K_j , $j \in \mathbb{N}$, ist ein affiner Unterraum von \mathbb{F}^n .

Jeder Klartext x aus einer solchen Nebenklasse K_j , $j \in \mathbb{N}$, lässt sich also wie folgt darstellen:

$$x = \kappa_j + x_{\mathcal{K}}, \quad x_{\mathcal{K}} \in \mathcal{K}.$$

Es soll nun wieder untersucht werden, welche Störung die Klartexte einer solchen Nebenklasse verursachen. Wird ein Klartext $x \in K_j$ von $Z \circ T$ abgebildet, so ergibt sich

$$\begin{aligned} (Z \circ T)(x) &= Ax + \beta' \\ &= A(\kappa_j + x_{\mathcal{K}}) + \beta' \\ &= A\kappa_j + \underbrace{Ax_{\mathcal{K}}}_{=0} + \beta' \\ &= A\kappa_j + \beta' \quad \forall x \in K_j. \end{aligned}$$

Somit ist offensichtlich, dass die Störung für jeden Klartext $x \in K_j$ für festes j wieder identisch ist, nämlich $p(A\kappa_j + \beta')$, da der für jeden einzelnen Klartext spezifische Anteil $x_{\mathcal{K}}$ nicht in die Störung eingeht. Nur der Repräsentant κ_j der Nebenklasse beeinflusst den Wert der Störung, dieser ist aber für alle Klartexte einer Nebenklasse gleich. Als Ergebnis lässt sich also festhalten, dass mit den beschriebenen Nebenklassen Klartextmengen gefunden wurden, die genau die eingangs gewünschten Eigenschaften bieten. Damit ist die Grundlage für diesen Angriff gegeben. Als nächstes werden nun noch einige Eigenschaften der Nebenklassen beschrieben.

4.2.3 Eigenschaften der Nebenklassen

Die folgenden Sätze ermöglichen Aussagen über die Nebenklassen, die für die Beurteilung des Angriffs relevant sind.

Satz 4.2.1. Sei \mathcal{K} wie oben definiert Untervektorraum von \mathbb{F}^n mit $|\mathbb{F}| = q$. Für die Dimension von \mathcal{K} gilt dann

$$\dim(\mathcal{K}) = n - r.$$

Beweis. \mathcal{K} ist der Kern der linearen Abbildung $(Z \circ T)_l$ in \mathbb{F}^n . Der Dimensionssatz der Linearen Algebra liefert nun

$$\dim(\mathcal{K}) = n - \text{rang}(Z \circ T)_l$$

T ist eine Bijektion, die Matrix M_T des linearen Teils von T hat also Rang n . Da die Abbildungen z_i , $i = 1, \dots, r$, aus Z linear unabhängig gewählt werden, hat die Matrix des linearen Teils von Z den Rang r . Folglich gilt

$$\text{rang}(Z \circ T)_t = r.$$

Damit folgt die Behauptung. \square

Satz 4.2.2. *Die Anzahl der Nebenklassen von \mathcal{K} ist q^r .*

Beweis. Für die Anzahl der Elemente von \mathcal{K} gilt mit Satz (4.2.1) $|\mathcal{K}| = q^{n-r}$. Da für $\kappa \in \mathbb{F}^n$ die Abbildung $g : \mathcal{K} \rightarrow \kappa + \mathcal{K} : x \mapsto \kappa + x$ eine Bijektion ist, folgt $|\kappa + \mathcal{K}| = |\mathcal{K}| = q^{n-r}$ für alle $\kappa \in \mathbb{F}^n$. Alle Nebenklassen haben also die gleiche Anzahl von q^{n-r} Elementen. Aus der Linearen Algebra ist bekannt, dass die diskunkte Vereinigung der Nebenklassen genau \mathbb{F}^n ist. Es gilt $|\mathbb{F}^n| = q^n$. Somit ist die Anzahl der disjunkten Nebenklassen q^r , denn $q^r \cdot q^{n-r} = q^n$. \square

Bemerkung. Für die beschriebenen disjunkten Nebenklassen $K_j = \kappa_j + \mathcal{K}$, $j = 0, \dots, q^r - 1$, gilt also

$$\mathbb{F}^n = \bigcup_{j=0}^{q^r-1} K_j.$$

Es können daher alle denkbaren Klartexte aus \mathbb{F}^n einer der Nebenklassen von \mathcal{K} zugeordnet werden. Somit ist auch für jeden Geheimtext ein Angriff möglich, es muss nur die Nebenklasse gefunden werden, in der der zugehörige Klartext liegt, um dann das entsprechende bilineare Gleichungssystem nach Patarin zu nutzen. Da aber die Parameter q und r bewußt klein gewählt werden (für Details siehe Abschnitt 3.6), ist somit auch die Anzahl der Nebenklassen klein, daher ist eine Suche hier effizient durchführbar.

Die Zugehörigkeit eines Klartextes $x \in \mathbb{F}^n$ zu einer bestimmten Nebenklasse kann über die bekannte Bedingung

$$a, b \in K_j \Leftrightarrow a - b \in K_0 = \mathcal{K}$$

für $j \in \{0, \dots, q^r - 1\}$ überprüft werden, indem $x = a$ und $\kappa_j = b$ gesetzt wird.

4.2.4 Zusammenfassung

Die vorangegangenen Überlegungen und Ergebnisse zeigen, dass bei Kenntnis des Kerns \mathcal{K} des linearen Teils der Abbildung $Z \circ T$ die Störung innerhalb der Perturbed Matsumoto Imai Chiffre soweit unwirksam gemacht werden kann, dass ein erfolgreicher Angriff auf das System durchgeführt werden kann. Indem \mathcal{K} bekannt ist und somit auch die Nebenklassen bestimmt werden können, kann ein Angreifer für die Klartexte jeder Nebenklasse mit dem öffentlichen Schlüssel die zugehörigen Geheimtexte erzeugen. Mit Hilfe dieser Klartext/Geheimtext-Paare kann er dann mit Patarins Angriff die nötigen Koeffizienten berechnen, um einen bilinearen Zusammenhang zwischen den Klar- und den Geheimtexten herstellen zu können. Das entstehende bilineare Gleichungssystem ist dabei immer nur für die Klartext/Geheimtext-Paare gültig, deren Klartexte in der Nebenklasse liegen, deren Elemente zur Berechnung der Koeffizienten dieses Gleichungssystems verwendet wurden. Im Unterschied zu Patarins klassischem

Angriff auf das C^* -System gibt es also nun mehrere bilineare Gleichungssysteme, und zwar für jede Nebenklasse eines. Aufgrund der geringen Anzahl von Nebenklassen gibt es entsprechend aber auch nur wenige derartige Gleichungssysteme, so dass das passende System für einen beliebigen Geheimtext mit akzeptablem Aufwand gefunden werden kann. Dies geschieht auf die gleiche Weise wie bei der Entschlüsselung: Es muss nur der Hashwert des vermuteten Klartexts mit der angehängten Prüfsumme aus der gefundenen Zeichenfolge verglichen werden (vgl. 3.4.2 (v)). Somit kann über die Korrektheit des Klartexts das richtige Gleichungssystem identifiziert werden. Da der Angriff keine weiteren Voraussetzungen erfordert, ist er auf jeden Geheimtext eines beliebigen Perturbed Matsumoto Imai Systems anwendbar. Die Durchführung ist effizient, zumal der aufwendigste Teil der Arbeit, das Auffinden des Kerns \mathcal{K} und das Aufstellen der q^r bilinearen Gleichungssysteme, nur einmal erfolgen muss. Die Entschlüsselung erfolgt dann einfach durch Lösen der Gleichungssysteme. Der Aufwand hierfür ist, verglichen mit Patarins klassischem Angriff auf ein C^* -System, nur um den Faktor q^r höher, da im Allgemeinen bis zu q^r Gleichungssysteme überprüft werden müssen. Nachdem diese Angriffsmethode somit hinreichend motiviert ist, stellt sich abschließend die Frage, wie der Kern \mathcal{K} berechnet werden kann. Da die Abbildung $Z \circ T$ für den Angreifer unbekannt ist, kann \mathcal{K} nicht auf konventionellem Weg berechnet werden. Es ist eine neue Methode notwendig, die sich als Voraussetzung nur mit dem öffentlichen Schlüssel des Systems sowie beliebigen Klartext/Geheimtext-Paaren begnügen muss. Ein Verfahren, das dies leistet, wurde von Fouque, Granboulan und Stern in [FGS05] als Grundlage für den Angriff auf die Perturbed Matsumoto Imai Chiffre vorgestellt. Genauer wurden zwei Methoden gefunden, die das Auffinden von \mathcal{K} ermöglichen können. Sie werden im nächsten Abschnitt erläutert.

4.3 Kryptoanalyse

Die zugrunde liegende Idee zur Konstruktion des Kerns \mathcal{K} basiert auf Erkenntnissen über einen Zusammenhang zwischen dem sogenannten Differential des öffentlichen Schlüssels des Perturbed Matsumoto Imai Systems und dem gesuchten Kern \mathcal{K} . Genauer besteht eine Beziehung zwischen der Dimension des Kerns des linearen Teils dieses Differentials und der Zugehörigkeit eines Eingavektors x zu \mathcal{K} . Als Ergebnis kann dieser Zusammenhang genutzt werden, um eine ausreichend große Anzahl von Vektoren aus \mathcal{K} zu finden, so dass \mathcal{K} rekonstruiert werden kann. Die entsprechenden Aussagen sind in einigen Theoremen enthalten, die im nächsten Abschnitt erläutert werden. Abschließend können mit Hilfe dieser Theoreme Methoden entwickelt werden, die eine systematische Rekonstruktion von \mathcal{K} ermöglichen. Vorab wird nun der Begriff des Differentials im Kontext der polynomiellen Abbildung des öffentlichen Schlüssels der Perturbed Matsumoto Imai Chiffre eingeführt.

4.3.1 Das Differential des öffentlichen Schlüssels

Die Beschreibung des Differentials erfolgt zunächst ganz allgemein. Sei \mathbb{F} wie bisher ein endlicher Körper mit q Elementen. Für jede Funktion $G : \mathbb{F}^n \rightarrow \mathbb{F}^m$ lässt sich das Differential als

$$dG_k(x) = G(x + k) - G(x), \quad k \in \mathbb{F}^n,$$

schreiben. Im Fall des öffentlichen Schlüssels der Perturbed Matsumoto Imai Chiffre ist G quadratisch, das Differential G ist also eine affin lineare Funktion. Schon an der Gestalt von G zeigt sich, dass die quadratischen Terme in x in der Differenz wegfällen. Wie bereits erwähnt, beziehen sich die entscheidenden Aussagen auf den linearen Teil des Differentials von G . Dieser sei daher folgendermaßen definiert:

Definition 4.3.1. Sei G ein Differential wie oben beschrieben. Dann wird die Abbildung

$$L_{G,k}(x) := dG_k(x) - dG_k(0)$$

als der lineare Teil von G bezeichnet.

Bemerkung. Für jede affin lineare Abbildung f gilt allgemein, dass $f(x) - f(0)$ linear ist, da in der Differenz gerade der konstante Teil (nämlich $f(0)$) der affin linearen Abbildung wegfällt.

$L_{G,k}$ lässt sich auch als bilineare Funktion

$$B_G(x, k) := L_{G,k}(x) = G(x + k) - G(x) - G(k) + G(0)$$

schreiben. Die Funktion B_G bzw. $L_{G,k}$ wird auch als Polarform bezeichnet.

Eigenschaften. Es werden nun einige Eigenschaften der Polarform gezeigt, die im weiteren Verlauf des Abschnitts verwendet werden. Seien dazu k und k' Elemente aus \mathbb{F}^n und seien G und G' Systeme quadratischer Polynome. Dann gelten folgende Aussagen:

1. $L_{G,k+k'} = L_{G,k} + L_{G,k'}$
2. $L_{G+G',k} = L_{G,k} + L_{G',k}$
3. $L_{G,k}(k) = 0$, falls die Charakteristik des Grundkörpers 2 ist.

$B_G(x, k) = L_{G,k}(x)$ ist eine bilineare Abbildung. Die erste Eigenschaft folgt daher aus der Linearität. Die zweite Eigenschaft folgt durch einfaches Nachrechnen, da $(G + G')(x) = G(x) + G'(x)$. Die dritte Eigenschaft lässt sich ebenfalls leicht einsehen. Denn mit Charakteristik 2 des Grundkörpers gilt

$$\begin{aligned} L_{G,k}(k) &= G(\underbrace{2k}_{=0}) - G(k) - G(k) + G(0) \\ &= \underbrace{2G(0)}_{=0} - \underbrace{2G(k)}_{=0} \\ &= 0. \end{aligned}$$

Mit diesen Begriffen ist es nun möglich, die bereits erwähnten Theoreme zu formulieren. Wie schon angesprochen, ist hierbei die entscheidende Größe die Dimension des Kerns des linearen Teils des Differentials, also $\dim(\ker L_{G,k})$. Für den Beweis des ersten Satzes werden zwei weitere Hilfssätze benötigt, die daher vorab präsentiert werden.

Hilfssatz 4.3.1. Seien q , i und n ganze Zahlen. Dann gilt folgender Zusammenhang:

$$\gcd(q^n - 1, q^i - 1) = q^{\gcd(n,i)} - 1.$$

Beweis. Mit Hilfe des Euklidischen Algorithmus, der hier nicht näher erläutert werden soll (Details in [Buc03]), lässt sich der größte gemeinsame Teiler zweier ganzer Zahlen a und b oder auch zweier Polynome berechnen. Der Algorithmus gibt dabei eine Folge von Zahlen aus, die folgende Gestalt hat: $(r_k)_{k \geq 0} = (r_0, r_1, \dots, r_{k_0}, 0, \dots)$. Für $a \geq b$ ist dabei $r_0 = a$, $r_1 = b$ und $r_{k_0} = \gcd(a, b)$, das heißt, der letzte Wert ungleich Null ist der gesuchte größte gemeinsame Teiler. Es sei nun $(r_k)_{k \geq 0}$ diese Folge. Mit den Bezeichnungen aus dem Hilfssatz gilt also

$$r_0 = n \text{ und } r_1 = i.$$

Sei nun k_0 die größte ganze Zahl, so dass $r_{k_0} \neq 0$. Dann gilt folglich

$$r_{k_0} = \gcd(n, i).$$

Sei darüber hinaus $(R_k)_{k \geq 0}$ die entsprechende Folge aus dem Euklidischen Algorithmus für die beiden Polynome

$$R_0 = X^n - 1 \text{ und } R_1 = X^i - 1,$$

in diesem Fall sei K_0 der Index, für den

$$R_{K_0} = \gcd(X^n - 1, X^i - 1)$$

gilt. Es soll nun durch Induktion gezeigt werden, dass die Behauptung

$$R_k = X^{r_k} - 1 \text{ für } 0 \leq k \leq k_0 + 1$$

gilt. Gilt die Aussage für das angegebene Intervall, ist sie allgemein gültig, da $r_k = r_{k_0+1}$ für $k \geq k_0 + 1$. Die Behauptung ist richtig für $k = 0$ und $k = 1$, denn es gilt $R_0 = X^n - 1 = X^{r_0} - 1$ sowie $R_1 = X^i - 1 = X^{r_1} - 1$. Sei nun $2 \leq k \leq k_0 + 1$. Beim Euklidischen Algorithmus gilt für die Glieder der Folge $(r_k)_{k \geq 0}$ der Zusammenhang

$$r_{k-2} = \alpha r_{k-1} + r_k, \quad \alpha \in \mathbb{N}.$$

Damit gilt aber

$$\begin{aligned} X^{r_{k-2}} - 1 &= \overbrace{(X^{r_{k-2}-r_{k-1}} + X^{r_{k-2}-2r_{k-1}} + \dots + X^{r_{k-2}-\alpha r_{k-1}})}{=: \beta} (X^{r_{k-1}} - 1) \\ &\quad + (X^{r_k} - 1) \\ &= \beta(X^{r_{k-1}} - 1) + (X^{r_k} - 1), \end{aligned}$$

wie man mit Hilfe des obigen Zusammenhangs durch Ausmultiplizieren der rechten Seite leicht nachrechnen kann. Folglich ist $X^{r_k} - 1$ der Rest bei der Division von $R_{k-2} = X^{r_{k-2}} - 1$ durch $R_{k-1} = X^{r_{k-1}} - 1$, da $r_k < r_{k-1}$. Also gilt $X^{r_k} - 1 = R_k$, das heißt, die Behauptung ist für den Index k richtig, sofern sie für $k - 1$ und $k - 2$ richtig war. Da, wie oben gezeigt, die Aussage für $k = 0$ und $k = 1$ wahr ist, folgt zusammen die Behauptung. Es gilt also $R_{k_0+1} = X^{r_{k_0+1}} - 1 = X^0 - 1 = 0$ und $R^{k_0} \neq 0$. Da im Euklidischen Algorithmus das Folgenglied mit dem größten Index k , das ungleich Null ist, gerade der größte gemeinsame Teiler ist, folgt also $K_0 = k_0$ und somit $R_{K_0} = R_{k_0} = X^{r_{k_0}} - 1 = X^{\gcd(n, i)} - 1$. Für $X = q$ folgt der Beweis des Hilfssatzes. \square

Hilfssatz 4.3.2. Sei \mathbb{E} ein endlicher Körper mit q^n Elementen und $X, A \in \mathbb{E}$. Dann hat die Gleichung

$$X^j = A$$

entweder keine Lösung oder die Anzahl der Lösungen ist $\gcd(j, q^n - 1)$.

Beweis. Die multiplikative Gruppe von \mathbb{E} hat $q^n - 1$ Elemente, da das neutrale Element der Addition (die Null) nicht enthalten ist. Es werden nun für den Beweis zwei Fälle unterschieden.

- (i) Im einfachen Fall ist $\gcd(j, q^n - 1) = 1$. Dann ist j invertierbar modulo $(q^n - 1)$. Sei nun h das Inverse von j , so dass also $hj \equiv 1 \pmod{q^n - 1}$. Erhebt man nun die Ausgangsgleichung $X^j = A$ zur h -ten Potenz, so erhält man

$$(X^j)^h = X^{jh} = X = A^h =: A'$$

In diesem Fall ist A' also die einzige Lösung der Gleichung.

- (ii) Sei andererseits $\gcd(j, q^n - 1) = d \neq 1$. Dann ist d ein Teiler von j und es existiert j' mit $j = dj'$ und $\gcd(j', q^n - 1) = 1$. Folglich ist j' invertierbar modulo $(q^n - 1)$ und es existiert ein h' mit $h'j' \equiv 1 \pmod{q^n - 1}$. Betrachtet man nun entsprechend die h' -te Potenz der Ausgangsgleichung, so folgt

$$(X^j)^{h'} = X^{dj'h'} = X^d = A^{h'}$$

Die Gleichung $X^d = A^{h'}$ kann nur Lösungen haben, wenn $A^{h'}$ eine d -te Potenz in \mathbb{E} ist. Ist dies nicht der Fall, ergibt sich gerade der Fall des Satzes, dass die Gleichung keine Lösung hat. Sei nun anderenfalls $A^{h'}$ eine d -te Potenz in \mathbb{E} . Es wird nun gezeigt, dass es dann genau d Lösungen gibt. Aus der Annahme, dass $A^{h'}$ eine d -te Potenz ist, also $A^{h'} \stackrel{!}{=} B^d$ mit $B \in \mathbb{E}$, folgt, dass mindestens eine Lösung existiert, nämlich $X = B$. In [BS96] ist ein Algorithmus von Adleman, Manders und Miller gegeben, mit dem mindestens eine Lösung gefunden werden kann. Die anderen Lösungen können dann berechnet werden, indem man die vorhandene Lösung mit den d -ten Einheitswurzeln aus \mathbb{E} multipliziert. Denn sei w eine solche Einheitswurzel und B eine Lösung. Dann ist auch $wB \neq B$ eine Lösung, denn es gilt

$$(wB)^d = w^d B^d = 1 \cdot B^d = A^{h'}$$

Abschließend muss nun noch gezeigt werden, dass es genau d solche Einheitswurzeln gibt. Da die multiplikative Gruppe eines endlichen Körpers zyklisch ist, existiert ein primitives Element g , das die Gruppe erzeugt. Dann ist das Element $g' = g^{\frac{q^n - 1}{d}}$ eine d -te Einheitswurzel, denn

$$(g')^d = g^{q^n - 1} = 1$$

nach dem kleinen Satz von Fermat. (Die Einheitswurzel g' ist dabei eine ganzzahlige Potenz von g , denn d teilt $q^n - 1$ nach Voraussetzung). Folglich sind aber auch die Elemente

$$w_i = (g')^i \text{ für } 1 \leq i \leq d \tag{4.3}$$

d -te Einheitswurzeln, denn für alle natürlichen Potenzen von g' gilt

$$((g')^i)^d = ((g')^d)^i = 1^i = 1.$$

Aber nur die d Potenzen aus dem in (4.3) erwähnten Intervall ergeben unterschiedliche Elemente. Denn da g ein Erzeuger der multiplikativen Gruppe von \mathbb{E} mit $q^n - 1$ Elementen ist, sind nur die Potenzen g^i für $1 \leq i \leq q^n - 1$ verschieden, höhere Potenzen nehmen zyklisch wieder die gleichen Werte an. Für die Einheitswurzeln

$$w_i = (g')^i = g^{(q^n - 1) \cdot \frac{i}{d}}$$

bedeutet dies aber gerade, dass nur die Potenzen für $1 \leq i \leq d$ tatsächlich verschiedene Werte ergeben, da der Exponent von g (im rechten Term) nur für dieses Intervall Werte aus $\{1, \dots, q^n - 1\}_{\mathbb{N}}$ annimmt. Damit sind die d gesuchten Einheitswurzeln bestimmt, folglich existieren in diesem Fall genau d Lösungen für die Ausgangsgleichung. □

Die beiden Hilfsätze ermöglichen nun den Beweis des nächsten Satzes, dessen Aussage zusammen mit den nachfolgenden Sätzen den Ansatz zur Konstruktion von \mathcal{K} liefert. Entscheidend ist hierbei die Dimension des Kerns des linearen Teils des Differentials, das hier zum einen beim C^* -System, zum anderen beim Perturbed Matsumoto Imai System betrachtet wird.

4.3.2 Theorem 1

Satz 4.3.1. *Sei P der öffentliche Schlüssel eines C^* -Systems der Dimension n über dem endlichen Körper \mathbb{F} mit q Elementen und Charakteristik 2. Der Exponent des geheimen inneren Polynoms P^* des Systems sei $q^\lambda + 1$. Sei $L_{P,k}$ wie oben beschrieben der lineare Teil des Differentials von P . Dann gilt*

$$\dim(\ker L_{P,k}) = \gcd(\lambda, n).$$

Beweis. Vorab sei daran erinnert, dass die Verschlüsselungsfunktion beim C^* -System folgende Gestalt hat: $P = S \circ \tilde{P} \circ T$, wobei P und \tilde{P} polynomielle Abbildungen in \mathbb{F}^n und S, T affin lineare Bijektionen sind (siehe (2.5)). S und T ändern somit die Dimension des Kerns von \tilde{P} nicht, es gilt also

$$\dim(\ker L_{P,k}) = \dim(\ker L_{\tilde{P},k}).$$

Sei darüber hinaus an die Transformation $\pi : \mathbb{E} \rightarrow \mathbb{F}^n$ (siehe (2.3)) erinnert, die zwischen dem Vektorraum \mathbb{F}^n über dem Grundkörper und dem Erweiterungskörper \mathbb{E} übersetzt. Sei nun $x = \pi(X)$ und $k = \pi(K)$. \tilde{P} ist die innere polynomielle Abbildung des C^* -Systems, das heißt $\tilde{P} = \pi \circ P^* \circ \pi^{-1}$ mit $P^* = X^{q^\lambda + 1}$ über \mathbb{E} . Der lineare Teil des Differentials lässt sich also schreiben als

$$L_{\tilde{P},k}(x) = \tilde{P}(x+k) - \tilde{P}(x) - \tilde{P}(k) + \tilde{P}(0) \quad (4.4)$$

$$= \pi[(X+K)^{q^\lambda+1} - X^{q^\lambda+1} - K^{q^\lambda+1}] \quad (4.5)$$

$$= \pi(X^{q^\lambda}K + XK^{q^\lambda}). \quad (4.6)$$

Der letzte Schritt lässt sich dabei leicht nachvollziehen, indem zum einen das Binom in (4.5) in die Binomische Reihe entwickelt wird und zum anderen beachtet wird, dass über \mathbb{E} $q^\lambda \equiv 0$ gilt, da q eine Potenz der Charakteristik ist und

daher kongruent zu Null ist:

$$\begin{aligned}
(X + K)^{q^\lambda + 1} &= \sum_{i=0}^{q^\lambda + 1} \binom{q^\lambda + 1}{i} X^{q^\lambda + 1 - i} K^i = \\
X^{q^\lambda + 1} &+ \underbrace{\binom{q^\lambda + 1}{1}}_{=\binom{1}{1}=1} X^{q^\lambda} K + \underbrace{\binom{q^\lambda + 1}{2}}_{=\binom{1}{2}=0} X^{q^\lambda - 1} K^2 + \dots \\
\dots &+ \underbrace{\binom{q^\lambda + 1}{q^\lambda - 1}}_{=\binom{1}{-1}=0} X^2 K^{q^\lambda - 1} + \underbrace{\binom{q^\lambda + 1}{q^\lambda}}_{=\binom{1}{0}=1} X K^{q^\lambda} + K^{q^\lambda + 1}.
\end{aligned}$$

Es ist leicht zu sehen, dass bis auf die ersten und die letzten beiden Terme der Binomischen Reihe alle anderen Summanden verschwinden, da ihre Binomialkoeffizienten Null sind. Es bleiben also nur vier Terme übrig, von denen der erste und der letzte in (4.5) noch subtrahiert werden, so dass sich (4.6) ergibt.

Es soll nun der Kern von $L_{\tilde{P},k}$ betrachtet werden. Für ein $x \neq 0$ aus \mathbb{F}^n gilt

$$x \in \ker L_{\tilde{P},k} \iff X^{q^\lambda} K + X K^{q^\lambda} = 0,$$

denn es gilt $x = \pi(X) = 0 \iff X = 0$, da π ein Isomorphismus ist. Die letzte Gleichung lässt sich folgendermaßen umschreiben:

$$X^{q^\lambda} K + X K^{q^\lambda} = X^{q^\lambda + 1} \left(\frac{K}{X} + \left(\frac{K}{X} \right)^{q^\lambda} \right) = 0.$$

Diese Schreibweise ist wohldefiniert, da $x \neq 0 \Rightarrow X \neq 0$ vorausgesetzt wurde. Aus dem selben Grund kann der erste Term der Gleichung, $X^{q^\lambda + 1}$, vernachlässigt werden, da er stets ungleich Null ist. Ersetzt man nun den Term $\frac{K}{X}$ zur Verbesserung der Übersicht durch Ω , so lässt sich die Gleichung also als

$$\Omega + \Omega^{q^\lambda} = 0, \quad \Omega \in \mathbb{E},$$

schreiben. Für $\Omega \neq 0$, was gleichbedeutend ist mit $K \neq 0$, lässt sich die Gleichung durch Ω teilen und es ergibt sich

$$\begin{aligned}
1 + \Omega^{q^\lambda - 1} &= 0 \\
\iff \Omega^{q^\lambda - 1} &= 1,
\end{aligned} \tag{4.7}$$

da unter der gegebenen Voraussetzung der Charakteristik 2 der Zusammenhang $1 + 1 = 0$, also $1 = -1$ gilt. Die Form dieser Gleichung entspricht der in Hilfssatz 4.3.2 verwendeten. Mit $\Omega = 1$ existiert eine Lösung der Gleichung. Aus Hilfssatz 4.3.2 folgt daher, dass die Gleichung $\gcd(q^\lambda - 1, q^n - 1)$ Lösungen besitzt. Mit Hilfssatz 4.3.1 folgt weiter, dass die Anzahl der Lösungen für Ω und damit auch für $x = \pi(X)$ mit $X = \frac{K}{\Omega}$ gerade $q^{\gcd(\lambda, n)} - 1$ ist. Da $L_{\tilde{P},k}$ eine lineare Abbildung ist, ist die Null, die für die letzten Überlegungen ausgeschlossen wurde und demnach nicht mitgezählt wurde, ebenfalls im Kern enthalten. Damit erhöht sich die Anzahl der Elemente im Kern auf $q^{\gcd(\lambda, n)}$. Da der Kern ein Vektorraum über dem Grundkörper \mathbb{F} mit $|\mathbb{F}| = q$ ist, folgt, dass die Dimension des Kerns gerade $\gcd(\lambda, n)$ ist. \square

Bemerkung. $\Omega = 1$ ist, wie bereits erwähnt, immer ein Lösung der Gleichung (4.7). Wegen $\Omega = \frac{K}{X}$ gilt dann $X = K$. Folglich ist $\pi(K) = k$ immer im Kern enthalten. Dies entspricht der dritten Eigenschaft von S. 36.

Die Bedeutung dieses Satzes wird erst im Zusammenspiel mit den folgenden Sätzen deutlich. Nachdem nun für das C^* -System eine Aussage über die Dimension des Kerns des linearen Teils des Differentials möglich ist, stellt sich die Frage, ob dies auch für das Perturbed Matsumoto Imai System möglich ist und von welchen Größen dieser Wert dort abhängig ist. Es wird sich zeigen, dass die Dimension tatsächlich davon abhängt, ob k in \mathcal{K} liegt oder nicht. Der Vergleich dieser Dimensionen lässt dann eine Aussage über die Zugehörigkeit eines Vektors zu \mathcal{K} zu und gibt somit einen Anhaltspunkt für die Konstruktion von \mathcal{K} .

4.3.3 Theorem 2

Satz 4.3.2. *Sei $\hat{P} = S \circ (\tilde{P} + \tilde{p}) \circ T$ der öffentliche Schlüssel des Perturbed Matsumoto Imai Systems, das durch Störung des C^* -Systems $P = S \circ \tilde{P} \circ T$ aus dem vorigen Satz entstanden ist. Sei $L_{\hat{P},k}$ wie oben beschrieben der lineare Teil des Differentials von \hat{P} . Weiterhin sei \mathcal{K} wie oben definiert. Dann gilt für $k \in \mathcal{K}$*

$$\dim(\ker L_{\hat{P},k}) = \gcd(\lambda, n).$$

Beweis. Es wird nun gezeigt, dass für $k \in \mathcal{K}$ die Aussage $L_{\hat{P},k} = L_{P,k}$ gilt. Mit dem vorigen Satz 4.3.1 folgt dann die Behauptung.

Betrachtet man nun daher die Differenz der beiden Polarformen, so ergibt sich mit Eigenschaft 1 von S. 36

$$\begin{aligned} L_{\hat{P},k}(x) - L_{P,k}(x) &= L_{\hat{P}-P,k}(x) \\ &= L_{S \circ (\tilde{P} + \tilde{p}) \circ T - S \circ \tilde{P} \circ T, k}(x) \\ &= \dots \end{aligned} \tag{4.8}$$

Mit der bereits definierten Schreibweise $S(x) = M_S x + v_S$, wobei $S_l(x) := M_S x$ der lineare Teil von S ist, gilt nun

$$\begin{aligned} (S \circ (\tilde{P} + \tilde{p}) \circ T)(x) &= M_S \tilde{P}(T(x)) + M_S \tilde{p}(T(x)) + v_S \\ &= (S \circ \tilde{P} \circ T)(x) + (S_l \circ \tilde{p} \circ T)(x). \end{aligned}$$

Damit lässt sich die Rechnung von (4.8) folgendermaßen fortsetzen:

$$\begin{aligned} \dots &= L_{S_l \circ \tilde{p} \circ T, k}(x) \\ &= (S_l \circ \tilde{p} \circ T)(x+k) - (S_l \circ \tilde{p} \circ T)(x) - (S_l \circ \tilde{p} \circ T)(k) + (S_l \circ \tilde{p} \circ T)(0) \\ &= 0. \end{aligned} \tag{4.9}$$

Der letzte Schritt kann dabei wie folgt nachvollzogen werden: Das Störungs-polynom \tilde{p} lässt sich wie gehabt schreiben als $\tilde{p} = p \circ Z$, also erhält man $S \circ \tilde{p} \circ T = S \circ p \circ Z \circ T$, wobei $Z \circ T$ die bereits bekannte affin lineare Abbildung ist. Für diese gilt aber nach (4.2)

$$(Z \circ T)(x+k) = A(x+k) + \beta' = Ax + \beta' = (Z \circ T)(x),$$

da nach Voraussetzung $k \in \mathcal{K}$ und somit $Ak = 0$ (vgl. Definition (4.2.1)). Damit gilt insbesondere auch

$$(Z \circ T)(k) = (Z \circ T)(0).$$

Folglich heben sich die ersten und letzten beiden Terme in (4.9) gegenseitig auf und die Differenz ergibt somit Null. Also gilt für $k \in \mathcal{K}$ tatsächlich $L_{\hat{P},k} = L_{P,k}$ und somit auch $\dim(\ker L_{\hat{P},k}) = \dim(\ker L_{P,k})$. Die Behauptung folgt nun aus Satz 4.3.1. \square

Interpretation

Der letzte Satz 4.3.2 macht schon einen höchst interessanten Zusammenhang deutlich, der über die Dimension des Kerns des Differential des öffentlichen Schlüssels eines Perturbed Matsumoto Imai Systems einen Rückschluss auf die Zugehörigkeit des Vektors k zu \mathcal{K} zulässt. Mit Satz 4.3.2 ist allerdings ausgehend von der Kenntnis der Dimension nur die Negation der Umkehraussage möglich, das heißt

$$\dim(\ker L_{\hat{P},k}) \neq \gcd(\lambda, n) \Rightarrow k \notin \mathcal{K}. \quad (4.10)$$

Somit lassen sich also Vektoren noch nicht als Elemente von \mathcal{K} entlarven, es lässt sich nur nachweisen, dass ein Vektor nicht in \mathcal{K} enthalten ist. Die nachweisbare Zugehörigkeit von Vektoren zu \mathcal{K} ist aber Voraussetzung, um diese Vektoren dann zur Rekonstruktion von \mathcal{K} verwenden zu können. Es sind also weitere Aussagen nötig. Der nächste Satz bringt dieses Ziel schon deutlich näher.

4.3.4 Theorem 3

Satz 4.3.3. *Sei \hat{P} der öffentliche Schlüssel eines Perturbed Matsumoto Imai Systems mit den gleichen Werten wie im vorigen Theorem 2 (Satz 4.3.2). Sei weiter $k \notin \mathcal{K}$. Dann gilt häufig*

$$\dim(\ker L_{\hat{P},k}) \neq \gcd(\lambda, n).$$

Bemerkung. Es ist unbedingt zu beachten, dass dieser Satz keine mathematisch eindeutige Aussage liefert. Die wünschenswerte Umkehraussage

$$\dim(\ker L_{\hat{P},k}) = \gcd(\lambda, n) \Rightarrow k \in \mathcal{K}$$

ist mit diesem Satz nicht möglich. Er gibt lediglich einen Hinweis darauf, dass die Korrektheit dieser Umkehraussage in vielen Fällen gegeben ist, jedoch nicht im Allgemeinen. Dieser entscheidende Unterschied hat daher einen großen Einfluss auf die weitere Verfahrensweise und die Methoden zur Rekonstruktion von \mathcal{K} , die auf Grundlage dieser Sätze nachfolgend entwickelt werden.

Empirischer Beweis. Die Aussage stützt sich auf experimentelle Ergebnisse. Zunächst folgen einige theoretische Überlegungen. Wie schon im Beweis von Satz 4.3.2 gilt

$$L_{\hat{P},k} = L_{P,k} + L_{S_I \circ P \circ Z \circ T, k}. \quad (4.11)$$

Nach Voraussetzung ist nun jedoch $k \notin \mathcal{K}$, es ist also im Allgemeinen

$$(Z \circ T)(x + k) \neq (Z \circ T)(x)$$

daher ist der zweite Summand $L_{S_l \circ p \circ Z \circ T, k}$ in (4.11) in diesem Fall nicht Null. Es handelt sich vielmehr um eine lineare Abbildung, deren Wert sich nahezu zufallsartig verhält, da er von für den Angreifer unbekanntem Klartexten abhängt. Die Dimension des Kerns von $L_{\hat{P}, k}$ ist daher in gleichem Maße zufallsartig und verhält sich entsprechend den Gesetzmäßigkeiten der Verteilung der Dimension des Kerns von zufälligen linearen Abbildungen.

Es ist allerdings tatsächlich möglich, etwas genauere Aussagen über die Dimension zu machen. So ist beispielsweise k immer im Kern von $L_{S_l \circ p \circ Z \circ T, k}$ enthalten, denn, wie schon in Eigenschaft 3 auf S. 36 gezeigt, gilt wegen Charakteristik 2

$$\begin{aligned} \underbrace{L_{S_l \circ p \circ Z \circ T, k}}_{=: Q}(k) &= \underbrace{Q(k+k)}_{=2k=0} - Q(k) - Q(k) + Q(0) \\ &= \underbrace{2Q(0)}_{=0} - \underbrace{2Q(k)}_{=0} \\ &= 0. \end{aligned}$$

Für $L_{P, k}$ gilt aber die entsprechende Aussage, das heißt $L_{P, k}(k) = 0$, wie auch bereits in der Bemerkung zu Satz 4.3.1 erläutert wurde. Daher ist k auch im Kern der Summe, also im Kern von $L_{\hat{P}, k}$ enthalten. Da k im Allgemeinen ungleich Null ist, ist die Dimension des Kerns also mindestens 1. Betrachtet man die Summe (4.11) erneut, so wird klar, dass alle Elemente, die im Kern der beiden Summanden auf der rechten Seite liegen, auch im Kern von $L_{\hat{P}, k}$ enthalten sind. Die Dimension dieses Kerns ist also mindestens so groß wie die Dimension des Schnitts der Kerne der beiden Summanden. Es wird daher nun die Dimension der Kerne dieser beiden Summanden untersucht.

Der erste Summand ist $L_{P, k}$. Aus Satz 4.3.1 ist bekannt, dass für die Dimension des Kerns $\dim(\ker L_{P, k}) = \gcd(\lambda, n)$ gilt. Der zweite Summand ist $L_{S_l \circ p \circ Z \circ T, k}$. Nach Satz 4.2.1 gilt $\dim(\ker(Z \circ T)) = \dim(\mathcal{K}) = n - r$. Damit folgt $\dim(\ker L_{S_l \circ p \circ Z \circ T, k}) = n - r$. Zwei Teilräume der Dimensionen $\gcd(\lambda, n)$ und $n - r$ eines Vektorraums der Dimension n haben einen Schnitt der Dimension $\gcd(\lambda, n) - r$, falls $\gcd(\lambda, n) > r$. In diesem Fall gibt es also mindestens $q^{\gcd(\lambda, n) - r}$ Vektoren im Kern von $L_{\hat{P}, k}$, da der dem besagten n -dimensionalen Vektorraum zugrunde liegende Körper \mathbb{F} die Mächtigkeit q hat.

Fouque, Granboulan und Stern konnten die Aussage dieses Satzes experimentell bestätigen, wie man in der Tabelle 4.1 sehen kann. \square

$\lambda = 41, n = 137, r = 6$			$\lambda = 40, n = 136, r = 6$		
Dimension	$k \in \mathcal{K}$	$k \notin \mathcal{K}$	Dimension	$k \in \mathcal{K}$	$k \notin \mathcal{K}$
1	1	$\approx \mathbf{0,59}$	3	0	$\approx 0,686$
>1	0	$\approx 0,41$	4	0	$\approx 0,290$
			5	0	$\approx 0,023$
			6	0	$\approx 5 \cdot 10^{-4}$
			7	0	$\approx 2 \cdot 10^{-6}$
			8	1	$\approx \mathbf{0}$
			>8	0	≈ 0

Tabelle 4.1: Experimentelle Häufigkeitsverteilung von $\dim(\ker L_{\hat{P}, k})$

Bemerkung. Für die Tabelle wurden die von Ding vorgeschlagenen Parameter verwendet, für die linke Tabelle gilt $\gcd(\lambda, n) = 1$, für die rechte $\gcd(\lambda, n) = 8$. Die Ergebnisse lassen sich folgendermaßen interpretieren: Die mittlere Spalte gibt an, mit welcher relativen Häufigkeit die entsprechende Dimension in der linken Spalte im Fall $k \in \mathcal{K}$ auftrat. Die Ergebnisse spiegeln gerade die Aussage von Satz 4.3.2 wieder, es tritt ausschließlich die Dimension $\dim(\ker L_{\hat{P},k}) = \gcd(\lambda, n)$ auf. In der rechten Spalte der Tabellen ist die relative Häufigkeit abzulesen, mit der im Falle $k \notin \mathcal{K}$ die in der linken Spalte angegebene Dimension vorlag. Es ist zu erkennen, dass für $k \notin \mathcal{K}$ tatsächlich eine hohe Häufigkeit für Dimensionen mit $\dim(\ker L_{\hat{P},k}) \neq \gcd(\lambda, n)$ zu verzeichnen war, wogegen die Häufigkeit des Auftretens von $\dim(\ker L_{\hat{P},k}) = \gcd(\lambda, n)$ geringer, in der rechten Tabelle sogar praktisch Null war. Dies bestätigt genau die Aussage des Satzes 4.3.3.

4.3.5 Zusammenfassung

Die Theoreme im letzten Abschnitt zeigen einen entscheidenden Zusammenhang zwischen der Dimension des Kerns des Differentials des öffentlichen Schlüssels eines Perturbed Matsumoto Imai Systems und der Zugehörigkeit eines Eingabevektors k zu \mathcal{K} . Mit Hilfe dieser Ergebnisse ist es nun möglich, Techniken zu entwickeln, die eine Rekonstruktion von \mathcal{K} erlauben. Ist diese Arbeit getan, lässt sich das System mit geeigneten Methoden angreifen, wie sie zu Beginn dieses Kapitels beschrieben wurden. Da die Sätze des letzten Abschnitts aber leider nur eine definitive Aussage darüber zulassen, ob ein Eingabevektor *nicht* in \mathcal{K} enthalten ist, nämlich

$$\dim(\ker L_{\hat{P},k}) \neq \gcd(\lambda, n) \Rightarrow k \notin \mathcal{K},$$

ist die Rekonstruktion von \mathcal{K} mit einem gewissen Aufwand verbunden, um ein zuverlässiges Ergebnis zu erhalten. Nähere Details finden sich im nächsten Abschnitt.

4.4 Rekonstruktion von \mathcal{K}

Um \mathcal{K} zu rekonstruieren, werden mindestens $\dim \mathcal{K}$ linear unabhängige Vektoren benötigt, die somit ein Erzeugendensystem von \mathcal{K} bilden. Die Grundlage für die abstrakte Entwicklung von Algorithmen liefert zunächst ein Testalgorithmus, der für einen gegebenen Vektor $x \in \mathbb{F}^n$ überprüfen kann, ob dieser *nicht* in \mathcal{K} enthalten ist. Sei T dieser Testalgorithmus. Dann ist

$$T(x) = 1 \text{ falls } \dim(\ker L_{\hat{P},x}) \neq \gcd(\lambda, n) \Rightarrow x \notin \mathcal{K}$$

und

$$T(x) = 0 \text{ falls } \dim(\ker L_{\hat{P},x}) = \gcd(\lambda, n) \Rightarrow x \in \mathcal{K} \text{ oder } x \notin \mathcal{K}.$$

Dieser Algorithmus basiert auf den Aussagen der Sätze im letzten Abschnitt. Zu beachten ist dabei, dass aufgrund der Tatsache, dass nur die Nicht-Zugehörigkeit eines Eingabevektors zu \mathcal{K} mit absoluter Sicherheit festgestellt werden kann, das Ergebnis des Testalgorithmus und damit auch das eines darauf basierenden Rekonstruktions-Algorithmus im Allgemeinen nur mit einer gewissen Wahrscheinlichkeit korrekt interpretiert werden kann:

Eine definitive Feststellung, dass ein gegebener Vektor in \mathcal{K} liegt, ist nicht möglich, daher kann die Ausgabe des Testalgorithmus im Fall $T(x) = 0$ nicht als absolut zuverlässig angesehen werden. Die Interpretation $T(x) = 0 \Rightarrow x \in \mathcal{K}$ ist vielmehr nur mit einer bestimmten Wahrscheinlichkeit korrekt. Denn dieser Fall geht auf den Satz 4.3.3 zurück, der hier leider keine verlässliche Aussage zulässt. Die Ausgabe $T(x) = 1$ dagegen kann als zuverlässig angesehen werden, da sie auf Satz 4.3.2 basiert, dessen Aussage eindeutig ist. Für Rekonstruktions-Algorithmen bedeutet dies, dass sie unter Berücksichtigung einer Einschätzung der Wahrscheinlichkeit der korrekten Interpretation der Ausgabe von T entwickelt sein müssen. Darauf basierend muss der Rekonstruktions-Algorithmus ein Ergebnis ausgeben, welches zumindest mit hoher Wahrscheinlichkeit korrekt ist, um einen erfolgreichen Angriff zu ermöglichen. Fouque, Granboulan und Stern haben zwei derartige Methoden vorgestellt, die auch kombiniert angewendet werden können. Sie werden in diesem Abschnitt vorgestellt.

4.4.1 Analyse des Testalgorithmus T

Als Grundlage wird zunächst eine Wahrscheinlichkeitsverteilung aufgestellt, die die möglichen Aussagen des Testalgorithmus T allgemein beschreibt. Es sei dazu

$$\alpha := \Pr[T(x) = 0] \quad (4.12)$$

die Wahrscheinlichkeit, dass der Testalgorithmus den Wert 0 ausgibt, das heißt, dass x in \mathcal{K} enthalten sein könnte oder aber auch nicht. Weiter sei

$$\beta := \Pr[x \in \mathcal{K}] \quad (4.13)$$

die Wahrscheinlichkeit, dass x tatsächlich in \mathcal{K} enthalten ist. Im Allgemeinen gilt $\alpha \geq \beta$, denn $\alpha = \Pr[T(x) = 0]$ deckt auch Fälle ab, in denen x nicht in \mathcal{K} enthalten ist, da $T(x) = 0$ keine eindeutige Aussage zulässt. Da $\dim \mathcal{K} = n - r$ und somit $|\mathcal{K}| = q^{n-r}$, gilt

$$\beta = \Pr[x \in \mathcal{K}] = \frac{q^{n-r}}{q^n} = q^{-r}.$$

Mit den obigen Definitionen lässt sich die Wahrscheinlichkeitsverteilung für die möglichen Ausgaben des Testalgorithmus T nun folgendermaßen schreiben:

	$x \in \mathcal{K}$	$x \notin \mathcal{K}$	Σ
$T(x) = 0$	β	$\alpha - \beta$	α
$T(x) = 1$	0	$1 - \alpha$	$1 - \alpha$
Σ	β	$1 - \beta$	1

Tabelle 4.2: Verteilung der Werte von T

Es gilt zu beachten, dass die Ausgabe $T(x) = 0$ berechtigten Anlass zur Interpretation $x \in \mathcal{K}$ gibt. Auch wenn die Korrektheit dieser Interpretation nicht gesichert ist, so ist es doch der einzige Anhaltspunkt. Die Problematik bei der Interpretation der Ergebnisse von T zeigt sich schon am Beispiel der Tabelle 4.1. Für $\gcd(\lambda, n) = 8$ (rechte Tabelle) treten in der entsprechenden fettgedruckten

Zeile praktisch keine Falschen Positiven auf, das heißt, es kommt praktisch nicht vor, dass, obwohl $k \notin \mathcal{K}$, die Dimension dennoch $\dim(\ker L_{\hat{P},k}) = \gcd(\lambda, n)$ ist, T hätte also nur selten „fälschlicherweise“ 0 ausgegeben und somit nur selten zur falschen Interpretation $x \in \mathcal{K}$ veranlasst. T hätte in diesem Fall also sehr zuverlässig gearbeitet. Bei $\gcd(\lambda, n) = 1$ (linke Tabelle) sieht es dagegen anders aus. Hier wurde in der entsprechenden Zeile in fast 60% aller Fälle mit $k \notin \mathcal{K}$ dennoch die Dimension $\dim(\ker L_{\hat{P},k}) = \gcd(\lambda, n)$ bestimmt. T hätte also in 60% der Fälle den Wert 0 ausgegeben, obwohl k nicht in \mathcal{K} enthalten war, und somit zu einer falschen Annahme verleitet. Damit wird deutlich, dass ein geeigneter Rekonstruktions-Algorithmus dieses Problem möglichst gut kompensieren muss, um ein verlässliches Ergebnis zu erzeugen.

Bemerkung. In den beiden nachfolgend vorgestellten Rekonstruktions-Methoden wird eine grundlegende Eigenschaft von \mathcal{K} benutzt. Wie für jeden Vektorraum gilt auch hier:

$$x, x' \in \mathcal{K} \Rightarrow x + x' \in \mathcal{K}. \quad (4.14)$$

Damit ist es leicht, aus vorhanden Elementen aus \mathcal{K} weitere zu berechnen.

4.4.2 Methode 1

Die zugrunde liegende Idee dieser Methode ist der folgende intuitive Ansatz: Falls für viele verschiedene $x' \in \mathcal{K}$ der Testalgorithmus T den Wert 0 ausgibt und ebenfalls $T(x + x') = 0$, dann gilt höchstwahrscheinlich auch $x \in \mathcal{K}$. Mit anderen Worten heißt das, wenn $T(x') = 0$ für viele verschiedene x' , wenn diese x' also wahrscheinlich in \mathcal{K} enthalten sind, und für jedes dieser x' zusätzlich auch $x + x'$ wahrscheinlich in \mathcal{K} enthalten ist, dann kann mit hoher Wahrscheinlichkeit davon ausgegangen werden, dass x ebenfalls in \mathcal{K} enthalten ist (vgl. (4.14)). Die Verlässlichkeit dieser Aussage steigt demnach mit der Anzahl der x' . Kurz gefasst lässt sich der Ansatz wie folgt formulieren:

$$\begin{aligned} (T(x') = 0 \text{ für viele } x') \wedge (T(x + x') = 0) \\ \implies (x \in \mathcal{K}). \end{aligned}$$

Die nun folgenden Überlegungen basieren auf der Annahme, dass für jedes feste x und ein zufällig gewähltes x' die Wahrscheinlichkeit, dass $T(x + x') = 0$ ist, unabhängig ist von der Wahrscheinlichkeit, dass $T(x') = 0$. Es gilt daher

$$\Pr[(T(x + x') = 0) \cap (T(x') = 0)] = \Pr[T(x + x') = 0] \cdot \Pr[T(x') = 0]. \quad (4.15)$$

Unter dieser Annahme soll nun die bedingte Wahrscheinlichkeit

$$\Pr_*(x) := \Pr[T(x + x') = 0 | T(x') = 0] \quad (4.16)$$

berechnet werden. Dies entspricht nach dem obigen Ansatz der Wahrscheinlichkeit, dass der Rekonstruktionsalgorithmus entscheidet, dieses x sei vermutlich in \mathcal{K} enthalten. Um einschätzen zu können, wie verlässlich die Ausgabe von T hierbei ist, werden nun zwei Fälle unter der Bedingung $T(x') = 0$ unterschieden. Zum einen wird untersucht, mit welcher Wahrscheinlichkeit $T(x + x') = 0$ für ein beliebiges x ausgegeben wird. Es wäre also möglich, dass dieses x nicht in \mathcal{K} enthalten ist, und T würde somit wieder zu einer falschen Annahme verleiten. Zum anderen wird die Wahrscheinlichkeit für $T(x + x') = 0$ für $x \in \mathcal{K}$ untersucht, das heißt die Wahrscheinlichkeit, dass T sich wie erwartet verhält und

zu einer korrekten Annahme führt. Die Differenz dieser beiden Werte soll einen Hinweis darauf geben, wie verlässlich die Ausgabe von T ist, um einschätzen zu können, wieviele Werte man mit T testen muss, bis man mit hoher Wahrscheinlichkeit genügend korrekte Ergebnisse erhalten hat. Die Idee wird weiter unten noch näher erläutert.

Fall 1: x ist zufällig gewählt

Für ein zufällig gewähltes x ist der Wert $x + x'$ für $T(x') = 0$ gleichverteilt. Mit (4.15) und (4.16) gilt

$$\begin{aligned} \Pr_*(x) &= \frac{\Pr[(T(x + x') = 0) \cap (T(x') = 0)]}{\Pr[T(x') = 0]} \\ &= \Pr[T(x + x') = 0] \\ &= \alpha, \end{aligned}$$

da hier sowohl x als auch $x + x'$ einfach als zufällige Elemente betrachtet werden, für die generell $\Pr[T(x) = 0] = \Pr[T(x + x') = 0] = \alpha$ gilt (vgl. (4.12)).

Fall 2: $x \in \mathcal{K}$

Betrachtet man jedoch speziell ein $x \in \mathcal{K}$, so ist der Wert von $T(x + x')$ nur noch von x' abhängig, da x nun fest ist. Es gibt also nur noch die beiden Fälle $x' \in \mathcal{K}$ und $x' \notin \mathcal{K}$ zu betrachten und damit gilt

$$\begin{aligned} \Pr_*(x) &= \Pr[x' \in \mathcal{K} | T(x') = 0] \cdot \Pr[T(x + x') = 0 | x + x' \in \mathcal{K}] \\ &\quad + \Pr[x' \notin \mathcal{K} | T(x') = 0] \cdot \Pr[T(x + x') = 0 | x + x' \notin \mathcal{K}]. \end{aligned}$$

Bemerkung. Diese Formel lässt sich folgendermaßen nachvollziehen: Nach (4.15) gilt $\Pr_*(x) = \Pr[T(x + x') = 0] \cdot \Pr[T(x') = 0]$. Allerdings gibt es in diesem speziellen Fall zwei Bedingungen zu beachten. Zum einen gilt $x \in \mathcal{K}$, zum anderen gilt nach wie vor $T(x') = 0$. Die Ausgabe $T(x + x') = 0$ kann generell unter zwei Bedingungen auftreten. Entweder $x + x' \in \mathcal{K}$ oder $x + x' \notin \mathcal{K}$. Daraus ergeben sich jeweils die zweiten Faktoren in den beiden Summanden der obigen Formel. Aber in diesem speziellen Fall treten diese beiden Ereignisse nur unter den vorab genannten Bedingungen auf. So tritt beispielsweise aufgrund von $x \in \mathcal{K}$ das Ereignis $x + x' \in \mathcal{K}$ nur auf, wenn $x' \in \mathcal{K}$ ist, wobei noch für dieses x' die Bedingung $T(x') = 0$ gelten muss. Das heißt, die Wahrscheinlichkeit beträgt gerade $\Pr[x' \in \mathcal{K} | T(x') = 0]$. Das erklärt den ersten Faktor des ersten Summanden der Formel, entsprechendes gilt für den zweiten Summanden.

Setzt man nun die Werte aus der Tabelle 4.2 in die Formel ein, so erhält man weiter

$$\Pr_*(x) = \frac{\beta}{\alpha} + \frac{\alpha - \beta}{\alpha} \cdot \frac{\alpha - \beta}{1 - \beta}.$$

Unter der vorsichtigen Annahme, dass der Testalgorithmus relativ oft $T(x) = 0$ ausgibt, obwohl $x \notin \mathcal{K}$, also $1 > \alpha \gg \beta > 0$, lässt sich der Term noch weiter

vereinfachen:

$$\begin{aligned} \frac{\Pr_*(x)}{\alpha} &= \frac{\beta}{\alpha^2} + \frac{(1 - \frac{\beta}{\alpha})^2}{1 - \beta} = \frac{\alpha^2 - 2\alpha\beta + \beta}{(1 - \beta)\alpha^2} \\ &= \frac{1 - \frac{2\beta}{\alpha} + \frac{\beta}{\alpha^2} + \beta - \beta}{1 - \beta} \\ &= \frac{1 - \beta + \beta(\frac{1}{\alpha^2} - \frac{2}{\alpha} + 1)}{1 - \beta} = 1 + \frac{\beta(\frac{1}{\alpha} - 1)^2}{1 - \beta} \\ &\approx 1 + \beta(\frac{1}{\alpha} - 1)^2, \end{aligned}$$

also

$$\Pr_*(x) \approx \alpha + \alpha\beta(\frac{1}{\alpha} - 1)^2.$$

Erwartungsgemäß ist der Wert $\Pr_*(x)$ für $x \in \mathcal{K}$ höher als im allgemeinen Fall. Wie schon oben erläutert, ist nun die Differenz der beiden Werte von \Pr_* für beliebiges x (Fall 1) bzw. $x \in \mathcal{K}$ (Fall 2) nun von Interesse. Sie gibt gerade an, mit welcher Wahrscheinlichkeit T zu einer falschen Annahme verleitet. Denn α gibt die Wahrscheinlichkeit an, mit der T allgemein für beliebige x den Wert 0 ausgibt, man also annimmt, x sei in \mathcal{K} enthalten, obwohl diese Annahme auch falsch sein kann. $\alpha + \alpha\beta(\frac{1}{\alpha} - 1)^2$ ist die Wahrscheinlichkeit für den Anteil darunter, wo x tatsächlich in \mathcal{K} enthalten war, wo T also sicher zu einer korrekten Annahme führt. Die Differenz entspricht daher der Irrtumswahrscheinlichkeit, dass T zwar 0 ausgibt, aber x doch nicht in \mathcal{K} enthalten war. Mit der Vereinfachung erhält man

$$\begin{aligned} \Pr_{*,x \in \mathcal{K}} - \Pr_{*,x \text{ beliebig}} &= \alpha + \alpha\beta(\frac{1}{\alpha} - 1)^2 - \alpha \\ &= \alpha\beta(\frac{1}{\alpha} - 1)^2, \end{aligned}$$

die Differenz ist folglich von der Ordnung $\alpha\beta$. Es ist also davon auszugehen, dass ein Anteil dieser Größe der Fälle, in denen $T(x + x') = 0$ bei $T(x') = 0$ gilt, dennoch fälschlicherweise zur Annahme führt, x sei in \mathcal{K} enthalten. Ergebnissen aus der Wahrscheinlichkeitstheorie entsprechend, lässt sich bei einer Anzahl von $N = \frac{1}{(\alpha\beta)^2}$ Vektoren x' mit $T(x') = 0$ mit relativ hoher Wahrscheinlichkeit eine korrekte Entscheidung treffen, ob x in \mathcal{K} enthalten ist oder nicht. Die Komplexität dieses Test beläuft sich auf β^{-2} . Fouque, Granboulan und Stern konnten diese Überlegungen experimentell bestätigen.

Jeder Vektor liegt mit einer Wahrscheinlichkeit $\beta = q^{-r}$ in \mathcal{K} , es werden also durchschnittlich mindestens q^r Vektoren benötigt, um überhaupt einen aus \mathcal{K} darunter zu haben. Diesen Vektor zu identifizieren, bedeutet mit obigem Algorithmus einen Aufwand von $\beta^{-2} = q^{2r}$. Darüber hinaus werden mindestens $n - r \approx n$ unterschiedliche Elemente von \mathcal{K} benötigt, um eine Basis zu finden. Die Komplexität für die Rekonstruktion von \mathcal{K} ist somit also nq^{3r} .

4.4.3 Methode 2

Diese Methode basiert auf einem graphen-theoretischen Ansatz, nämlich dem Problem, in einem Graphen eine möglichst große Clique zu finden. Es wird ein

Graph definiert, dessen Punkte gerade die Elemente x sind, für die $T(x) = 0$ gilt, die also potentiell in \mathcal{K} enthalten sein könnten. Für je zwei dieser Punkte x und x' wird $T(x + x')$ berechnet. Ist die Ausgabe $T(x + x') = 0$, werden diese beiden Punkte mit einer Kante verbunden. Das bedeutet, dass gerade im Fall $T(x + x') = 0$ mit $T(x') = 0$, also dem Fall, der wie oben zur Annahme führt, x sei in \mathcal{K} enthalten, eine Kante existiert. Insbesondere sind alle Punkte $x \in \mathcal{K}$ miteinander in dieser Weise verbunden, da für zwei Punkte a und b aus \mathcal{K} sowohl $T(a) = T(b) = 0$ als auch $T(a + b) = 0$ gilt, da auch $a + b \in \mathcal{K}$. Sie sind in einer sogenannten großen Clique. Betrachtet man nun einen Punkt x , der mit sehr vielen anderen Punkten x' durch eine Kante verbunden ist, so ist die Wahrscheinlichkeit also relativ groß, dass dieser Punkt x in \mathcal{K} enthalten ist. Indem man nach einer möglichst großen Clique, einer Gruppe von Punkten, die alle miteinander verbunden sind, sucht, kann man folglich \mathcal{K} oder zumindest einen möglichst großen Teil der Elemente von \mathcal{K} finden.

Dazu muss nicht unbedingt der gesamte Graph konstruiert werden. In der Praxis werden N Punkte verwendet. Auch hier besteht natürlich wieder das Interesse, $n - r$ Punkte zu finden, die zu linear unabhängigen Elementen aus \mathcal{K} gehören, da somit eine Basis von \mathcal{K} gefunden wäre. Da für die Wahrscheinlichkeit, dass ein beliebiges x in \mathcal{K} enthalten ist, gerade $\Pr[x \in \mathcal{K}] = \beta$ gilt, sind unter $N > \frac{n}{\beta}$ Punkten wahrscheinlich n Punkte aus \mathcal{K} dabei, daher muss N mindestens so groß gewählt werden. Unter den N Elementen werden nun einige durch Prüfen von $T(x + x') \stackrel{?}{=} 0$ miteinander verbunden. Innerhalb der N Punkte entsteht so also eine Clique, die mindestens die besagten $\beta N > n$ Elemente aus \mathcal{K} enthält. Es wird nun wie oben (vgl. (4.15)) die Annahme gemacht, dass $T(x) = 0$ und $T(x + x') = 0$ unabhängige Ereignisse sind. Dann hat allgemein ein derartiger Graph αN^2 Kanten, denn jeder der N Punkte wird mit αN der anderen Punkte verbunden, da es unter der Annahme der Unabhängigkeit wegen

$$\Pr[T(x + x') = 0] = \Pr[T(x) = 0] = \alpha$$

gerade αN Punkte x' gibt, so dass $T(x + x') = 0$ ausgegeben wird. Die Kanten zwischen Punkten, die nicht in \mathcal{K} enthalten sind, sind zufällig verteilt.

Ergebnisse aus dem Bereich der Graphentheorie sagen aus, dass eine Clique C_{max} maximaler Größe in einem zufälligen Graphen, der aus N Punkten besteht und in dem die Wahrscheinlichkeit für eine Kante α ist, ungefähr aus

$$|C_{max}| \approx \frac{2 \log N}{\log \frac{1}{\alpha}} + O(\log \log N)$$

Punkten besteht (siehe [Bol01, S. 282f.]). Zusammengefasst bedeutet das folgendes: Ein Graph aus N Punkten x mit $T(x) = 0$ enthält ungefähr βN Punkte aus \mathcal{K} . Eine Clique maximaler Größe in diesem Graphen enthält ungefähr $|C_{max}|$ Elemente. Diese Elemente sind höchstwahrscheinlich aus \mathcal{K} , da für je zwei Elemente x, x' dieser Clique $T(x + x') = 0$ gilt. Dennoch sind neben den βN Elementen aus \mathcal{K} auch noch weitere Elemente in dieser Clique, die nicht aus \mathcal{K} sind, da die Ausgaben von T eben nicht völlig zuverlässig sind. Es gilt also allgemein $\beta N \leq |C_{max}|$. Wenn nun aber

$$\beta N \approx |C_{max}|, \quad (4.17)$$

dann bedeutet dies, dass die größte Clique fast ausschließlich aus den βN Elementen besteht, die wirklich aus \mathcal{K} stammen. Der Anteil der Elemente, die zwar

in der Clique sind, aber *nicht* aus \mathcal{K} stammen, ist in diesem Fall also extrem gering. Wählt man daher N entsprechend wie in (4.17) und sucht mittels verfügbarer Algorithmen die größte Clique, so hat man mit sehr großer Wahrscheinlichkeit nahezu ausschließlich Elemente aus \mathcal{K} gefunden. Mit diesen Elementen lässt sich \mathcal{K} dann rekonstruieren.

4.5 Durchführung des Angriffs

Der in diesem Kapitel beschriebene Angriff lässt sich grob in zwei Abschnitte einteilen. Bevor ein Geheimtext konkret entschlüsselt werden kann, muss zunächst der Raum \mathcal{K} bestimmt werden. Dies kann in der Praxis durch eine Kombination der beiden oben erwähnten Rekonstruktions-Algorithmen erreicht werden. Anschließend können dann die affinen Nebenklassen von \mathcal{K} berechnet werden. Für jede der Nebenklassen kann dann mit Hilfe des Angriffs von Patarin ein bilineares Gleichungssystem aufgestellt werden, das einen linearen Zusammenhang zwischen den Geheimtexten und den zugehörigen Klartexten aus den jeweiligen Nebenklassen herstellt. Mit Hilfe dieser Gleichungssysteme kann dann ein gegebener Geheimtext entschlüsselt werden. Jedes Gleichungssystem führt für einen gegebenen Geheimtext zu einem anderen Urbild, es liegen also für einen Geheimtext immer mehrere Urbilder vor. Da vorab unbekannt ist, aus welcher affinen Nebenklasse der korrekte Klartext stammt, muss dieser daher mit Hilfe von Redundanzen in der Menge der Urbilder identifiziert werden.

4.6 Fazit

Der beschriebene Angriff nutzt eine verhältnismäßig tief liegende technische Schwäche des Perturbed Matsumoto Imai Systems aus, denn der entscheidende Zusammenhang zwischen der Dimension des Kerns des linearen Teils des Differentials des öffentlichen Schlüssels und dem Kern \mathcal{K} des linearen Teils der Abbildung $Z \circ T$ und insbesondere die Konsequenzen dieses Zusammenhangs sind sicher nicht gerade offensichtlich. Dennoch basiert der eigentliche Angriff nach der Rekonstruktion des Kerns \mathcal{K} auf einem alten bekannten Verfahren, dem Angriff von Patarin. In Anbetracht der Tatsache, dass die Perturbed Matsumoto Imai Chiffre unter anderem als Reaktion auf genau diesen Angriff von Patarin auf die C^* -Chiffre entstanden ist, ist es umso erstaunlicher, dass dennoch gerade dieser Angriff auch bei der modifizierten Chiffre noch Anwendung findet. Zwar bedarf es mitunter einer genaueren Analyse, um eine wirklich zuverlässige Rekonstruktion von \mathcal{K} zu gewährleisten, da immer eine Fehlerwahrscheinlichkeit existiert, die nur durch eingehende Tests für ein System genauer kalkuliert werden kann. Es können aber doch vorab Parameter festgelegt werden, die mit großer Wahrscheinlichkeit zu zuverlässigen Ergebnissen führen. Der differentielle Angriff ist somit eine sehr wirkungsvolle Bedrohung der Perturbed Matsumoto Imai Chiffre. Das System stellt als Modifikation der C^* -Chiffre insgesamt zwar einen interessanten Ansatz dar, der aber noch nicht ausreicht, um das System wirklich sicher zu machen. Um dies zu erreichen, muss das System so modifiziert werden, dass die angesprochene Schwäche nicht mehr als Angriffsziel dienen kann. Es darf nicht möglich sein, allein durch die Kenntnis des öffentlichen Schlüssels Rückschlüsse auf \mathcal{K} ziehen zu können, wodurch das System

dann angreifbar wird. Diesen Ansatz verfolgt PMI+, eine neue Modifikation der Perturbed Matsumoto Imai Chiffre.

Kapitel 5

Die PMI+ Chiffre

5.1 Einleitung

Die Perturbed Matsumoto Imai Chiffre wurde als Modifikation der C^* -Chiffre unter anderem mit dem Ziel konstruiert, resistent gegen Patarins Angriff zu sein. Wie im letzten Kapitel deutlich wurde, ist die Perturbed Matsumoto Imai Chiffre zwar in dieser Hinsicht vielversprechend, konnte aber leider dennoch gebrochen werden. Die Schwachstelle des Systems resultiert aus einem Zusammenhang zwischen dem Differential des öffentlichen Schlüssels und dem Raum $\mathcal{K} \subseteq \mathbb{F}^n$, der mit Hilfe des Differentials rekonstruiert werden kann und damit einen Angriff auf das System ermöglicht. In einem neuen Ansatz (vgl. [DG05]) wurde versucht, den genannten Zusammenhang so zu verschleiern, dass eine Rekonstruktion von \mathcal{K} nicht mehr möglich ist. Die neue Modifikation geht dabei sehr gezielt vor. Es wurde genau analysiert, wo die Ursachen für die Angreifbarkeit liegen und systematisch ein Konzept entwickelt, das exakt diese Schwachstellen behebt. Das neue System kann somit als sehr konsequente Weiterentwicklung der Perturbed Matsumoto Imai Chiffre bezeichnet werden.

Konkret wird der öffentliche Schlüssel eines Perturbed Matsumoto Imai Systems um einige zusätzliche Polynome erweitert, sie werden als +-Polynome bezeichnet. Diese Störung lässt sich im Gegensatz zur internen Störung der Perturbed Matsumoto Imai Chiffre als extern bezeichnen, da nicht die bereits verwendeten Variablen verändert werden, sondern neue Komponenten hinzugefügt werden. Die externe Störung hat zur Folge, dass die Dimension des Kerns des linearen Teils des Differentials des öffentlichen Schlüssels, also $\dim(\ker L_{\hat{p}+,x})$, für fast alle Klartexte $x \in \mathbb{F}^n$ gleich ist. Das bedeutet, dass der Testalgorithmus T , auf dessen Ausgabe die Rekonstruktion von \mathcal{K} aufbaut, fast immer den selben Wert ausgibt. Damit ist eine Entscheidung, ob $x \in \mathcal{K}$ oder $x \notin \mathcal{K}$, nicht mehr möglich. Eine Rekonstruktion von \mathcal{K} ist somit verhindert und ein differentieller Angriff auf ein PMI+-System nutzlos. PMI+ widersteht damit allen bisher bekannten Angriffen auf C^* und die Perturbed Matsumoto Imai Chiffre.

5.2 Idee

Der Erfolg des differentiellen Angriffs auf die Perturbed Matsumoto Imai Chiffre liegt darin begründet, dass der Testalgorithmus T in der Lage ist, verschiedene

Fälle zu unterscheiden, da mit einer gewissen Wahrscheinlichkeit unterschiedliche Werte für den Defekt des linearen Teils des Differentials, $L_{\hat{P},x}$, vorliegen, je nachdem, ob x in \mathcal{K} enthalten ist oder nicht. Um den differentiellen Angriff abzuwehren, muss also ein Szenario geschaffen werden, in dem nahezu jeder Vektor x des Klartextraums zum selben Defekt der Abbildung $L_{\hat{P},x}$ führt. Der Testalgorithmus T gäbe dann unabhängig von der Zugehörigkeit eines Vektors x zu \mathcal{K} fast immer den gleichen Wert aus. Basierend auf diesen Werten ist dann keine Entscheidung über die Zugehörigkeit zu \mathcal{K} mehr möglich und \mathcal{K} kann somit nicht rekonstruiert werden.

Dieser Effekt wird bei PMI+ durch eine Erweiterung des öffentlichen Schlüssels um zusätzliche quadratische Polynome erreicht. Es zeigt sich, dass diese Polynome den Defekt der linearen Abbildung $L_{\hat{P},x}$ beeinflussen. Denn betrachtet man $L_{\hat{P},x}$ in Matrix-Darstellung, so wird klar, dass das Hinzufügen von weiteren Polynomen im öffentlichen Schlüssel zu weiteren Zeilen in dieser Matrix führt. Das bedeutet aber, dass sich der Rang der Abbildung damit erhöhen kann, was gleichbedeutend mit einer Verringerung des Defekts ist. Bei ausreichender Anzahl an neuen Polynomen wird so ein Zustand erreicht, in dem der Defekt des linearen Teils des Differentials für fast alle Vektoren x des Klartextraums identisch ist, unabhängig davon, ob x in \mathcal{K} enthalten ist oder nicht. Genauer wird der Defekt für fast alle Vektoren des Klartextraums auf den Wert 1 reduziert. Nähere Details zur genauen Funktionsweise dieses Konzepts werden später in diesem Kapitel vorgestellt.

5.3 Funktionsweise der PMI+-Chiffre

Wie oben erläutert verhindert die PMI+-Chiffre den differentiellen Angriff durch Hinzufügen von zusätzlichen Polynomen zum öffentlichen Schlüssel. Diese Modifikation hat zur Folge, dass der Defekt der Abbildung $L_{\hat{P},x}$ für nahezu alle Elemente x des Klartextraums identisch ist, wodurch eine Rekonstruktion von \mathcal{K} verhindert wird. Sei nun \hat{P} der öffentliche Schlüssel eines Perturbed Matsumoto Imai Systems. Es gilt also

$$\hat{P}(x_1, \dots, x_n) := (S \circ \bar{P} \circ T)(x_1, \dots, x_n),$$

wie in (3.3) und (3.4) definiert. Dabei sind wie gehabt S und T affin lineare Abbildungen und $\bar{P} = (\bar{P}_1, \dots, \bar{P}_n)^t$ die innere polynomielle Abbildung des Systems. Diese wird nun modifiziert. Dazu werden zunächst a zufällige quadratische Polynome definiert:

$$q_i(x_1, \dots, x_n), \quad i = 1, \dots, a. \quad (5.1)$$

Mit Hilfe dieser neuen Polynome wird nun die innere polynomielle Abbildung des PMI+-Systems wie folgt festgelegt:

$$\bar{P}^+ : \mathbb{F}^n \rightarrow \mathbb{F}^{n+a} \quad (5.2)$$

mit

$$\bar{P}^+ = (\bar{P}_1, \dots, \bar{P}_n, q_1, \dots, q_a)^t. \quad (5.3)$$

Die affine Abbildung S muss an die größere Dimension des Bildraums von \bar{P}^+ angepasst werden. Es sei also

$$S^+ : \mathbb{F}^{n+a} \rightarrow \mathbb{F}^{n+a} \quad (5.4)$$

eine zufällig gewählte invertierbare affin lineare Abbildung des PMI+-Systems. Damit lässt sich nun der öffentliche Schlüssel eines PMI+-Systems folgendermaßen schreiben:

$$\hat{P}^+ : \mathbb{F}^n \rightarrow \mathbb{F}^{n+a} \quad (5.5)$$

mit

$$\hat{P}^+(x_1, \dots, x_n) = (S^+ \circ \bar{P}^+ \circ T)(x_1, \dots, x_n) = (\hat{y}_1^+, \dots, \hat{y}_{n+a}^+) \quad (5.6)$$

Der öffentliche Schlüssel eines PMI+-Systems besteht also aus $n + a$ quadratischen Polynomen über \mathbb{F}^n . Die ersten n Polynome des inneren MQ -Systems \bar{P}^+ sind identisch mit denen des entsprechenden Perturbed Matsumoto Imai Systems.

5.3.1 Ver- und Entschlüsselung mit PMI+

Verschlüsselung

Die Verschlüsselung eines Klartextes läuft nach dem gleichen Prinzip wie bei der Perturbed Matsumoto Imai Chiffre ab. Auf einen Klartext $(x_1, \dots, x_n) \in \mathbb{F}^n$ wird die polynomielle Abbildung des öffentlichen Schlüssels \hat{P}^+ angewendet. Das Ergebnis ist der Geheimtext $(\hat{y}_1^+, \dots, \hat{y}_{n+a}^+)$, der im Vergleich zur Perturbed Matsumoto Imai Chiffre um a Stellen länger ist. Interessant ist vielmehr die Entschlüsselung, da hier nicht nur größere Unterschiede im Vergleich zum Ablauf beim Perturbed Matsumoto Imai System bestehen, sondern darüber hinaus auch noch ein neuer Effekt auftritt, der sich bei der Entschlüsselung sinnvoll nutzen lässt. Der Aufwand wird dadurch positiv beeinflusst.

Entschlüsselung

Bei der Entschlüsselung muss zunächst die affin lineare Abbildung S^+ invertiert werden. Anschließend werden vom erhaltenen Vektor die letzten a Komponenten entfernt, da diese bei der Verschlüsselung durch die zusätzlichen PMI+-Polynome entstanden sind. Sie sind also zur weiteren Rekonstruktion des Klartexts nicht erforderlich. Die nächsten Schritte werden nun analog zum Entschlüsselungsvorgang bei der Perturbed Matsumoto Imai Chiffre vorgenommen.

Wie bereits erwähnt, kann bei der Entschlüsselung noch ein Begleiteffekt von PMI+ genutzt werden. Bei einem Perturbed Matsumoto Imai System hat jeder Geheimtext bis zu q^r verschiedene Urbilder. Nur eins davon ist jedoch der Klartext, so dass dieser noch in der Menge der Urbilder identifiziert werden muss. Dies geschieht für gewöhnlich durch zusätzliche Redundanzen, beispielsweise mit Prüfsummen, die gemeinsam mit dem Klartext verschlüsselt werden (vgl. Abschnitt 3.4.2 (v)). Bei PMI+ lassen sich hierfür jedoch die zusätzlichen +-Polynome verwenden. Nach der Multiplikation des Geheimtexts mit $(S^+)^{-1}$ liegt der Vektor $(\bar{P}_1, \dots, \bar{P}_n, q_1, \dots, q_a)$ vor. Aus $(\bar{P}_1, \dots, \bar{P}_n)$ werden nun die

Urbilder berechnet. Bei der Verschlüsselung ging aber der Klartext auch in die +-Polynome (q_1, \dots, q_a) ein. Unter den gefundenen Urbildern muss es also eines geben, das genau diese Werte für die +-Polynome erzeugt hat, nämlich den Klartext. Das entsprechende Urbild kann somit korrekt identifiziert werden, ohne dass zusätzliche Mittel nötig würden. Es muss nur das Urbild gesucht werden, das zu den entsprechenden Werten (q_1, \dots, q_a) führt. Die Funktionsweise von PMI+ unterscheidet sich also nur geringfügig von der des Perturbed Matsumoto Imai Systems. Dennoch hat die Modifikation einen weitreichenden Einfluss auf die Sicherheit des Systems, wie im folgenden Abschnitt deutlich wird.

5.4 Die Auswirkungen der +-Modifikation

Wie in der Einleitung bereits erwähnt wurde, wurde PMI+ konsequent entwickelt, um einen differentiellen Angriff, wie er im letzten Kapitel beschrieben wird, zu verhindern. Der Ansatz hierfür ist, den Defekt der Abbildung $L_{\hat{P},x}$, also $\dim(\ker L_{\hat{P},x})$, durch die Modifikation so zu beeinflussen, dass er für nahezu alle Vektoren x aus dem Klartextrraum gleich groß ist. Der Testalgorithmus T kann dann nicht mehr entscheiden, ob ein Vektor aus \mathcal{K} stammt oder nicht, \mathcal{K} kann also nicht rekonstruiert werden, und der Angriff ist somit verhindert.

Festlegung

Es wird zunächst der Fall

$$\gcd(\lambda, n) = 1 \tag{5.7}$$

betrachtet. Die Verallgemeinerung erfolgt in einem späteren Abschnitt.

5.4.1 Analyse des Defekts von $L_{\hat{P}^+,x}$

Im Fall $\gcd(\lambda, n) = 1$ gilt bei einem klassischen Perturbed Matsumoto Imai System nach Satz 4.3.2 für den Defekt von $L_{\hat{P},x}$, dass

$$\dim(\ker L_{\hat{P},x}) = 1 \quad \text{für alle } x \in \mathcal{K}.$$

Nach Satz 4.3.3 gilt dann weiter, dass

$$\dim(\ker L_{\hat{P},x}) \neq 1 \quad \text{für viele } x \notin \mathcal{K}.$$

Dieser Umstand, den der Testalgorithmus T ausnutzt, soll nun geändert werden. Die Modifikation muss das System dabei so verändern, dass im entstehenden PMI+-System auch

$$\dim(\ker L_{\hat{P}^+,x}) = 1 \quad \text{für fast alle } x \notin \mathcal{K}$$

gilt. Um den Effekt der +-Polynome besser beschreiben zu können, wird die lineare Abbildung $L_{\cdot,x}$ im weiteren Verlauf nun als Matrix betrachtet. Es sei also $M_{x,0}$ die Matrix, die die Abbildung $L_{\hat{P},x}$ beschreibt. Weiter sei $M_{x,a}$ die Matrix, die die entsprechende Abbildung $L_{\hat{P}^+,x}$ beschreibt, bei der das PMI+-System aus dem Perturbed Matsumoto Imai System durch Hinzufügen von a +-Polynomen entstanden ist. Es soll nun untersucht werden, welchen Einfluss

die +-Polynome auf den Defekt der Abbildung $L_{\cdot,x}$ bzw. der Matrix $M_{x,\cdot}$ haben. Nach dem Dimensionssatz aus der Linearen Algebra gilt im vorliegenden Fall

$$\dim(\ker L_{\cdot,x}) + \dim(\operatorname{im} L_{\cdot,x}) = n$$

und daher

$$\operatorname{defekt}(L_{\cdot,x}) = n - \operatorname{rang}(L_{\cdot,x}).$$

Da Rang und Defekt einer linearen Abbildung also in direktem Zusammenhang stehen, wird im weiteren Verlauf der Rang der Matrix $M_{x,\cdot}$ untersucht, da direkte Aussagen über den Defekt anhand der Matrix hier ungünstig sind. Mit Hilfe des Dimensionssatzes werden dann sofort die gewünschten Aussagen über den Defekt der Matrix ermöglicht.

Sei also $R(a)$ der Rang der Matrix $M_{x,a}$:

$$R(a) := \operatorname{rang} M_{x,a}.$$

Zunächst lässt sich festhalten, dass $R(a) < n$, denn der Defekt von $M_{x,a}$ ist größer Null, da wegen der geforderten Charakteristik 2 des Grundkörpers

$$L_{\hat{p}^+,x}(x) = 0$$

und somit auch

$$M_{x,a}x^t = 0 \tag{5.8}$$

gilt (vgl. Eigenschaft 3 auf S. 36). Der Kern hat also im Allgemeinen mindestens Dimension 1. Das Hinzufügen eines +-Polynoms zum öffentlichen Schlüssel des Perturbed Matsumoto Imai Systems resultiert in einer zusätzlichen Zeile in der Matrix $M_{x,0}$, die damit zu $M_{x,1}$ wird. Dadurch kann sich der Rang der Matrix um 1 erhöhen, falls die neue Zeile linear unabhängig von den anderen Zeilen ist. Anderenfalls bleibt der Rang des alten Systems erhalten. Es hängt also von der Wahl des +-Polynoms ab, ob der Rang sich erhöht oder nicht. Zur Erinnerung: Ziel ist, dass sich der Rang durch Hinzufügen einer bestimmten Anzahl von +-Polynomen so erhöht, dass der Defekt für möglichst viele $x \notin \mathcal{K}$ auf den Wert 1 verringert wird. Es wird nun also die Wahrscheinlichkeit betrachtet für das gewünschte Ereignis, dass sich der Rang durch Hinzufügen eines +-Polynoms erhöht. Dieses Ereignis beschreibt den Übergang von einem PMI+-System mit a +-Polynomen zu einem mit $a + 1$ +-Polynomen. Gesucht ist also

$$\Pr[R(a+1) = R(a) + 1].$$

Es ist zu beachten, dass diese Wahrscheinlichkeit für $R(a) = n - 1$ Null ist, da $R(a) < n$, wie oben erläutert. Sei also

$$R(a) = n - i, \quad i = 2, \dots, n - 1.$$

In dieser Darstellung entspricht wegen des Dimensionssatzes i gerade dem Defekt der Matrix $M_{x,a}$. Das Hinzufügen eines +-Polynoms erzeugt nur dann eine Erhöhung des Rangs der Matrix, wenn der neue Zeilenvektor in der Matrix zwei Bedingungen erfüllt:

1. Der neue Zeilenvektor muss orthogonal zu x sein. Denn wie schon erwähnt, gilt auch hier $L_{\widehat{P}^+,x}(x) = 0$ wegen Charakteristik 2. Das neue +-Polynom wird zwar beliebig gewählt, aber dies gilt nicht für die entsprechende neue Zeile in der Matrix, da in diese u.a. noch x eingeht. Sie ist eher als ein Resultat der Wahl des +-Polynoms und x zu sehen. Auch der neue Zeilenvektor in der entsprechenden Matrix $M_{x,a+1}$ muss also orthogonal zu x sein, damit die eben erwähnte Eigenschaft bestehen bleibt (vgl. (5.8)). x spannt einen eindimensionalen Unterraum von \mathbb{F}^n auf. Der Orthogonalraum, aus dem der neue Zeilenvektor stammen muss, hat also die Dimension $n - 1$ und enthält wegen $|\mathbb{F}| = q$ somit q^{n-1} Elemente.
2. Damit sich der Rang der Matrix erhöht, muss der neue Zeilenvektor von den Zeilen aus $M_{x,a}$ linear unabhängig sein. Nach Voraussetzung hat die Matrix $M_{x,a}$ vor dem Hinzufügen des neuen Zeilenvektors den Rang $n - i$, $i = 2, \dots, n - 1$. Der von den Zeilenvektoren aufgespannte Raum hat somit die Dimension $n - i$ und enthält q^{n-i} Elemente. Der neue Zeilenvektor darf nicht in diesem Raum enthalten sein.

Ein geeigneter neuer Zeilenvektor muss beide Bedingungen erfüllen. Die Wahrscheinlichkeit dafür lässt sich wie folgt bestimmen. Aus der Menge der Zeilenvektoren, die Bedingung 1 erfüllen (das sind q^{n-1} Vektoren), werden die ausgewählt, die Bedingung 2 erfüllen. Das bedeutet aber, dass diese Zeilenvektoren *nicht* im Span der Zeilenvektoren der Matrix $M_{x,a}$ enthalten sein dürfen. Es ist dabei leichter, zunächst das Gegenereignis zu berechnen, dass also der neue Zeilenvektor in dem genannten Span enthalten ist. Die Wahrscheinlichkeit hierfür ist

$$\frac{q^{n-i}}{q^{n-1}} = q^{1-i}.$$

Das gesuchte Gegenereignis, das schließlich die Erhöhung des Rangs um 1 durch Hinzufügen eines +-Polynoms beschreibt, hat also die Wahrscheinlichkeit

$$\Pr[R(a+1) = R(a) + 1] = 1 - q^{1-i}, \quad i = 2, \dots, n - 1. \quad (5.9)$$

Es ist zu beachten, dass dieses Ereignis gleichbedeutend ist mit der Verringerung des Defekts um 1.

Die Häufigkeitsverteilung des Defekts

Die bisherigen Überlegungen beziehen sich nur auf ein spezielles $x \in \mathbb{F}^n$. Ziel ist jedoch, eine Aussage für mehrere Vektoren zu machen, da der Defekt für möglichst viele Vektoren $x \notin \mathcal{K}$ verändert werden soll. Es sei daher $n_{\delta,a}$ die Anzahl der Vektoren x , die den Defekt

$$\dim(\ker M_{x,a}) = \delta, \quad \delta = 1, \dots, n - 1,$$

zur Folge haben. Dann gilt folgender rekursiver Zusammenhang:

$$n_{\delta,a+1} = n_{\delta,a} \cdot q^{1-\delta} + n_{\delta+1,a} \cdot (1 - q^{-\delta}) \quad (5.10)$$

Es ist zu erkennen, dass bei geeigneter Wahl von a erreicht werden kann, dass $n_{\delta,a+1}$ deutlich größer ist als $n_{\delta,a}$ oder insbesondere $n_{\delta,0}$. Letzterer Wert entspricht gerade dem klassischen Perturbed Matsumoto Imai System. Hier umfasst

$n_{\delta,0}$ beispielsweise für $\delta = \gcd(\lambda, n)$ alle $x \in \mathcal{K}$ und einige wenige weitere. $n_{\delta,a+1}$ hingegen beschreibt den Fall PMI+, der dann weitaus mehr Vektoren umfasst als \mathcal{K} , was genau die erwünschte Konsequenz hat, dass $x \in \mathcal{K}$ und $x \notin \mathcal{K}$ vom Testalgorithmus T nicht mehr klar unterschieden werden können.

Bemerkung. Der Zusammenhang (5.10) lässt sich folgendermaßen nachvollziehen: Beim Übergang eines Systems mit a +-Polynomen auf ein System mit $a+1$ +-Polynomen gibt es zwei mögliche Konsequenzen. Da das hinzugekommene +-Polynom zufällig gewählt wurde, ist nicht klar, ob es die obigen Bedingungen erfüllt oder nicht. Somit ist nicht klar, ob der Defekt der Matrix $M_{x,a+1}$ verkleinert werden konnte oder nicht. Es muss daher der Erwartungswert für $n_{\delta,a+1}$ berechnet werden. Dieser setzt sich aus beiden möglichen Fällen zusammen: Zum einen kann der erwünschte Fall eintreten, dass der Rang der Matrix vergrößert und damit der Defekt verkleinert wird. Dies passiert, wenn das hinzugefügte +-Polynom den beschriebenen Bedingungen genügt. Dann ist $n_{\delta,a+1}$ gerade die Anzahl der Vektoren x , die vor dem Hinzufügen des neuen +-Polynoms den Defekt $\delta+1$ der Matrix $M_{x,a}$ zur Folge hatten, das waren $n_{\delta+1,a}$ viele. Die Wahrscheinlichkeit hierfür ist im betrachteten Fall

$$1 - q^{1-(\delta+1)} = 1 - q^{-\delta}.$$

Zum anderen besteht die Möglichkeit, dass der Defekt der Matrix durch Hinzufügen des neuen +-Polynoms nicht verändert wird. Dann entspricht $n_{\delta,a+1}$ gerade der Anzahl $n_{\delta,a}$ der Vektoren, die schon vorher den Defekt δ verursacht haben. Der Rang bzw. Defekt ändert sich also nicht. Dieser Fall entspricht gerade dem Gegenereignis von (5.9) und tritt daher mit der Wahrscheinlichkeit

$$1 - (1 - q^{1-\delta}) = q^{1-\delta}$$

auf. Für den Erwartungswert der Anzahl von Vektoren x im neuen PMI+-System, die den Defekt $\dim(\ker M_{x,a+1}) = \delta$ verursachen, ergibt sich also der Zusammenhang (5.10). Die Beschreibung der Situation mittels eines Erwartungswertes lässt sich auch dahingehend verstehen, dass die betrachtete Matrix immer nur für einen bestimmten Vektor x betrachtet wird. Bezogen auf den gesamten Klartextrraum werden also die durch das Hinzufügen von +-Polynomen möglichen Effekte immer alle auftreten. Das heißt, bei einigen Vektoren werden die neuen +-Polynome einen reduzierenden Effekt in Bezug auf den Defekt der Matrix haben, bei anderen hingegen nicht. Der zu erwartende Schnitt, also der Erwartungswert, ist daher die entscheidende Größe.

Um nun eine Aussage darüber machen zu können, wieviele +-Polynome nötig sind, um ein Perturbed Matsumoto Imai System hinreichend gegen differentielle Angriffe zu schützen, muss die Verteilung von $n_{\delta,a}$ in Abhängigkeit von a betrachtet werden. Es muss dabei ein Szenario beschrieben werden, dass für $n_{\delta,a}$ einen Ausgangswert, eine Initialverteilung besitzt. Dieser entspricht dem Perturbed Matsumoto Imai System ohne zusätzliche +-Polynome ($a=0$). Weiter muss jeder Übergang zu einem PMI+ System mit wachsender Anzahl an +-Polynomen Schritt für Schritt betrachtet werden können. Ein ideales technische Hilfsmittel zur Beschreibung dieses Szenarios sind die sogenannten Markov-Ketten.

5.4.2 Das Markov-Modell

Um die Wahrscheinlichkeiten für den Übergang eines Systems mit a +-Polynomen auf ein System mit $a+1$ +-Polynomen zu beschreiben, wird beim Markov-Modell eine spezielle Matrix verwendet. Jeder Eintrag in der Matrix beschreibt dabei die Übergangswahrscheinlichkeit von einem Zustand s_i zu einem Zustand s_j , wobei i und j gerade den Zeilen- bzw. Spaltenposition in der Matrix entsprechen. Wendet man dieses Modell auf das vorliegende Szenario an, so ergibt sich folgendes.

Beschreibung der Übergangsmatrix \mathcal{P}

Sei \mathcal{P} eine $(n \times n)$ -Matrix mit Einträgen (p_{ij}) von folgender Gestalt:

$$p_{ij} = \begin{cases} q^{1-i}, & \text{für } i = j; \\ 1 - q^{1-i}, & \text{für } i = j + 1; \\ 0, & \text{sonst.} \end{cases} \quad (5.11)$$

Die Einträge der Matrix sind folgendermaßen zu verstehen: Seien s_i und s_j zwei Zustände des PMI+-Systems. s_i , $i = 1, \dots, n$, beschreibt dabei den Zustand, dass für festes x der Defekt der Matrix $M_{x,a}$ gerade i ist:

$$s_i \quad : \iff \quad \dim(\ker M_{x,a}) = i, \quad i = 1, \dots, n.$$

Ein Eintrag p_{ij} beschreibt also die Wahrscheinlichkeit, dass das System durch Hinzufügen eines +-Polynoms für ein festes x vom Defekt i der Matrix $M_{x,a}$ zum Defekt j der Matrix $M_{x,a+1}$ übergeht. Natürlich kann der Defekt im Zustand s_j nur $j = i - 1$ oder $j = i$ sein, je nachdem, ob das Hinzufügen des +-Polynoms den Rang der Matrix $M_{x,a+1}$ erhöht hat oder nicht. Da x immer im Kern von $M_{x,a}$ enthalten ist und der Defekt somit immer mindestens 1 ist, kann also der Zustand s_1 nicht verlassen werden, da ein niedrigerer Defekt nicht möglich ist. Ein solcher Zustand wird im Markov-Modell als *Absorptionszustand* bezeichnet. Die anderen Zustände s_i für $i = 2, \dots, n$ hingegen werden *Übergangszustände* genannt. Da im vorliegenden Szenario jedoch mehrere +-Polynome sukzessiv hinzugefügt werden, ist der folgende Zusammenhang von Bedeutung. Ein m -stufiger Übergang, also eine Übergang von einem Zustand s_i zu einem Zustand s_j in m Schritten, wird durch die Matrix

$$\mathcal{P}_m := \mathcal{P}^m \quad (5.12)$$

beschrieben. Hier können sich i und j dann natürlich auch um mehr als 1 unterscheiden. Die Korrektheit dieser Aussage lässt sich durch einfaches Nachrechnen leicht überprüfen. Somit lässt sich nun mittels der Matrix \mathcal{P}_a das Hinzufügen von a +-Polynomen beschreiben. Es fehlt nur noch die Verteilung für den Initialzustand, also den Zustand des Perturbed Matsumoto Imai Systems, das als Ausgangspunkt der Untersuchung betrachtet wird.

Beschreibung des Initialzustands

Die Übergangsmatrix \mathcal{P} beschreibt die Wahrscheinlichkeit, mit der sich durch das Hinzufügen eines +-Polynoms der Defekt der Matrix $M_{x,\cdot}$ von einem Zustand zu einem anderen ändert. Darüber hinaus ist also noch ein Startwert

nötig, der den Zustand vor dem Hinzufügen der +-Polynome beschreibt. Auch der Defekt der entsprechenden Matrix $M_{x,0}$ ist gemäß einer spezifischen Funktion verteilt. Dieser sogenannte Initialzustand soll nun beschrieben werden. Zunächst sei \mathcal{M}_x die Matrix, die $L_{P,x}$, den linearen Teil des Differentials eines klassischen C^* -Systems, beschreibt. \mathcal{M}_x stellt also für einen gegebenen Vektor x im Fall eines C^* -Systems die Analogie zur Matrix $M_{x,0}$ im Fall eines Perturbed Matsumoto Imai Systems dar. Nach Satz 4.3.1 gilt für den Defekt der Matrix \mathcal{M}_x

$$\text{defekt } \mathcal{M}_x = \dim(\ker \mathcal{M}_x) \stackrel{!}{=} \gcd(\lambda, n) = 1$$

nach Voraussetzung (5.7). Ausgehend von der Kenntnis des Defekts beim C^* -System soll nun der Defekt der entsprechenden Matrix $M_{x,0}$ des Perturbed Matsumoto Imai Systems analysiert werden, indem verfolgt wird, welche Auswirkungen die Perturbed Matsumoto Imai Modifikation auf den Defekt der Matrix \mathcal{M}_x des C^* -Systems hat. Konkret wird wieder der Rang der Matrizen untersucht, um dann mit Hilfe des Dimensionssatzes auf den Defekt zu schließen.

Im betrachteten Fall $\gcd(\lambda, n) = 1$ ist der Defekt der Matrix \mathcal{M}_x für das C^* -System gleich 1, also gilt für den Rang

$$\text{rang } \mathcal{M}_x = n - 1.$$

Die Matrix \mathcal{M}_x hat also $n - 1$ linear unabhängige Spalten. Dieses C^* -System

$$P(x) = (S \circ \tilde{P} \circ T)(x), \quad x \in \mathbb{F}^n,$$

wird nun modifiziert, so dass das Perturbed Matsumoto Imai System

$$\hat{P}(x) = (S \circ (\tilde{P} + (p \circ Z)) \circ T)(x)$$

entsteht. Es wird dabei ein spezieller Fall eines Perturbed Matsumoto Imai Systems betrachtet, der aber die allgemeine Gültigkeit der resultierenden Aussagen nicht beschränkt, wie im Anschluss gezeigt wird. Sei also die affin lineare Abbildung T des Systems so gewählt, dass für einen beliebigen Klartext $x = (x_1, \dots, x_n)^t$ die Ausgabe der Abbildung Z nur noch eine Funktion in x_1, \dots, x_r ist. Um die spezielle Wahl kenntlich zu machen, wird diese Abbildung im Folgenden T' genannt. Es gilt also

$$(Z \circ T') \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} z_1 \\ \vdots \\ z_r \end{pmatrix},$$

wobei die Funktionen z_1, \dots, z_r jeweils nur noch von x_1, \dots, x_r abhängig sind (vgl. Abschnitt 3.2). Die restlichen Komponenten des Klartextvektors gehen aufgrund der speziellen Wahl von T' nicht mehr ein, da deren Koeffizienten in der affinen Abbildung $Z \circ T'$ Null sind. Entscheidend ist nun, dass dann natürlich die Störpolynome $p(z_1, \dots, z_r)$ ebenfalls nur noch Polynome in x_1, \dots, x_r sind. Das bedeutet aber in weiterer Konsequenz für die Abbildung $L_{\hat{P},x}$ des entstandenen Perturbed Matsumoto Imai Systems im Vergleich zu $L_{P,x}$ aus dem C^* -System, dass durch die Störung nur die Koeffizienten der Terme geändert werden, die eine der Komponenten x_1, \dots, x_r enthalten. Dies ist leicht einzusehen, wenn man die Eigenschaften der Abbildung $L_{.,x}$ betrachtet (vgl. S. 36): Es gilt

$$L_{\tilde{P}+p \circ Z, x} = L_{\tilde{P}, x} + L_{p \circ Z, x}. \quad (5.13)$$

Der erste Summand der rechten Seite in (5.13) ist zeilenweise von der Form $\sum_{j=1}^n \mu_{ij} x_j$, der zweite von der Form $\sum_{j=1}^r \nu_{ij} x_j$ mit Koeffizienten $\mu_{ij}, \nu_{ij} \in \mathbb{F}$, $i = 1, \dots, n$. Addiert man diese beiden Summen, so ergeben sich nur in den ersten r Termen neue Koeffizienten. In der Darstellung der Abbildung $L_{\cdot, x}$ als Matrix $M_{x, \cdot}$ bedeutet dies, dass nur die ersten r Spalten der Matrix \mathcal{M}_x durch die Addition der Störpolynome geändert werden. Der Rang der Matrix \mathcal{M}_x des C^* -Systems ist $n - 1$, der Defekt ist 1 (vgl. (5.7)). Der Übergang zur Matrix $M_{x,0}$ des Perturbed Matsumoto Imai Systems, das heißt die Störung der ersten r Spalten der Matrix \mathcal{M}_x , kann nach den vorangegangenen Überlegungen mit einem Austausch der ersten r Spalten gegen r zufällige neue Spalten beschrieben werden, zumal die Störpolynome zufällig gewählt werden. Um die Auswirkungen dieses Vorgangs auf den Rang der Matrix zu untersuchen, werden nun zwei Schritte betrachtet: Zuerst werden r Spalten der Matrix \mathcal{M}_x entfernt. Dadurch verringert sich der Rang der Matrix um r oder $r - 1$, je nachdem, ob die r entfernten Spalten aus der Menge der $n - 1$ linear unabhängigen Spalten von \mathcal{M}_x stammen oder ob auch die eine linear abhängige Spalte darunter ist. Beide Ereignisse treten mit unterschiedlicher Wahrscheinlichkeit auf:

Verringerung des Rangs um r : Dieser Fall tritt ein, wenn r linear unabhängige Spalten von \mathcal{M}_x entfernt werden. Die Wahrscheinlichkeit für dieses Ereignis ist

$$\frac{\binom{n-1}{r}}{\binom{n}{r}} = 1 - \frac{r}{n}.$$

Der Defekt der Matrix wird dabei um r auf den Wert $r + 1$ vergrößert.

Verringerung des Rangs um $r - 1$: Dieser Fall tritt ein, wenn sich unter den r entfernten Spalten neben $r - 1$ linear unabhängigen auch die eine linear abhängige Spalte befand. Die Wahrscheinlichkeit für dieses Ereignis ist

$$\frac{\binom{n-1}{r-1}}{\binom{n}{r}} = \frac{r}{n}.$$

Der Defekt der Matrix wird dabei um $r - 1$ auf den Wert r vergrößert.

Dieser Zustand lässt sich durch den $(r + 1)$ -komponentigen Vektor π_0 darstellen:

$$\pi_0 = \underbrace{\left(0, \dots, 0, \frac{r}{n}, 1 - \frac{r}{n}\right)^t}_{r+1 \text{ Komponenten}}.$$

Wie in der Übergangsmatrix \mathcal{P} beschreibt die i -te Komponente des Vektors π_0 gerade die Wahrscheinlichkeit für den Zustand s_i mit dem Defekt i für $i = 1, \dots, r + 1$.

Die Auswirkung des Störvorgangs durch die Perturbed Matsumoto Imai Modifikation auf den Defekt der Matrix wird nun weiter beschrieben, indem im zweiten Schritt wieder r Spalten zur Matrix hinzugefügt werden. Da die Störpolynome, die bei der Perturbed Matsumoto Imai Modifikation zu den bisherigen Polynomen des C^* -Systems addiert werden, zufällig gewählt werden, ist die Änderung der Spalten der Matrix \mathcal{M}_x des C^* -Systems beim Übergang zur Matrix $M_{x,0}$ des Perturbed Matsumoto Imai Systems ebenso zufällig. Es werden daher zur korrekten Beschreibung des Vorgangs r zufällig gewählte Spalten hinzugefügt.

Die so entstehende Matrix entspricht genau der Matrix $M_{x,0}$ eines Perturbed Matsumoto Imai Systems, das aus dem zu Beginn gewählten C^* -System hervorgegangen ist. Da die neuen Spalten zufällig gewählt werden, kann nicht vorhergesagt werden, ob sie linear unabhängig von den bereits vorhandenen Spalten der Matrix sind oder nicht. Daher kann auch die Auswirkung auf den Rang bzw. den Defekt der Matrix nicht mit Sicherheit angegeben werden. Allerdings lässt sich diese Auswirkung gerade mit der Matrix \mathcal{P} beschreiben, die oben für das Hinzufügen der a +-Polynome beim Übergang zum PMI+-System aufgestellt wurde. Denn das Hinzufügen einer Spalte hat die gleichen Konsequenzen wie das Hinzufügen einer Zeile. Da aber der Defekt durch das Hinzufügen von Spalten höchstens verringert, nicht jedoch vergrößert werden kann, sind Zustände mit einem Defekt größer $r + 1$ nicht möglich. Die Wahrscheinlichkeitsverteilung für den Defekt, der durch das Hinzufügen der Spalten ausgehend vom Zustand mit Defekt $r + 1$ bzw. r entsteht, wird daher mit der Matrix \mathcal{P}_r beschrieben. Dabei ist \mathcal{P}_r die Matrix, die sich aus dem $(r + 1) \times (r + 1)$ -Block oben links aus der Matrix \mathcal{P} zusammensetzt. Aus dem gleichen Grund wird auch der Vektor π_0 nur in $r + 1$ Komponenten dargestellt. Wie schon die Matrix \mathcal{P} beschreibt natürlich auch die Matrix \mathcal{P}_r nur das Hinzufügen einer einzigen Spalte. Der gesamte Vorgang des sukzessiven Hinzufügens von r Spalten wird daher entsprechend der Formel (5.12) mit der Matrix \mathcal{P}_r^r beschrieben.

5.4.3 Wahrscheinlichkeitsverteilung des Defekts

Im Initialzustand

Zusammengefasst kann nun die Wahrscheinlichkeitsverteilung des Defekts des Initialzustands, der durch die Matrix $M_{x,0}$ beschrieben wird, aufgestellt werden. Der Ausdruck setzt sich aus den beiden oben erläuterten Schritten zusammen. Zunächst werden r Spalten der Matrix M_x des zugrunde liegenden C^* -Systems entfernt, was einen Defekt von r oder $r + 1$ zur Folge hat. Anschließend wird der Defekt durch das sukzessive Hinzufügen von r zufälligen Spalten gemäß der Wahrscheinlichkeiten aus der Matrix \mathcal{P}_r^r wieder verringert. Somit ergibt sich folgender Zusammenhang für die Wahrscheinlichkeitsverteilung des Defekts im Initialzustand, der von der Matrix $M_{x,0}$ beschrieben wird:

$$\pi_0 \mathcal{P}_r^r = \begin{pmatrix} \Pr[\text{defekt}(M_{x,0}) = 1] \\ \vdots \\ \Pr[\text{defekt}(M_{x,0}) = r + 1] \end{pmatrix}. \quad (5.14)$$

Als Beispiel sei hier die Wahrscheinlichkeitsverteilung für den Initialzustand eines Perturbed Matsumoto Imai System mit den Parametern $n = 31$ und $r = 6$ gegeben (vgl. [DG05]):

$$\pi_0 \mathcal{P}_6^6 = \begin{pmatrix} 0,350125 \\ 0,539086 \\ 0,106813 \\ 3,94582 \times 10^{-3} \\ 3,01929 \times 10^{-5} \\ 4,67581 \times 10^{-8} \\ 1,17354 \times 10^{-11} \end{pmatrix}.$$

Im PMI+-System

Um nun schließlich die gewünschte Wahrscheinlichkeitsverteilung für den Defekt des PMI+-Systems zu erhalten, muss also bei a zusätzlichen +-Polynomen die Verteilung gemäß

$$\pi_0 \mathcal{P}_r^r \mathcal{P}_r^a = \pi_0 \mathcal{P}_r^{r+a} \quad (5.15)$$

berechnet werden. Mit Hilfe dieser Verteilung lässt sich nun erkennen, welchen Effekt das Hinzufügen der +-Polynome auf den Defekt der Matrix $M_{x,0}$ hat, so dass abgeschätzt werden kann, wieviele +-Polynome nötig sind, um den Defekt auf den eingangs des Abschnitts gewünschten Wert 1 für möglichst viele Vektoren $x \notin \mathcal{K}$ zu bringen. Vor einer Betrachtung der experimentell gewonnenen Daten zur weiteren Auswertung muss aber zunächst noch der bisher betrachtete Fall einer Störung in r Spalten verallgemeinert werden.

5.4.4 Verallgemeinerung der Wahl von T

Die Überlegungen des letzten Abschnitts beziehen sich durchgehend auf eine Störung der Matrix \mathcal{M}_x in r Spalten, da vorausgesetzt wurde, dass die affine Abbildung T so gewählt wird, dass für einen Klartext $x = (x_1, \dots, x_n)^t$ die Abbildung Z nur noch eine Funktion in den Variablen x_1, \dots, x_r darstellt. Tatsächlich stellt diese spezielle Wahl der Abbildung T aber keine Einschränkung der Allgemeinheit dar, wie im Folgenden veranschaulicht wird.

Wie schon im letzten Abschnitt angedeutet wurde, ist es immer möglich, die Abbildung T entsprechend zu wählen. Im Folgenden sei diese speziell gewählte Abbildung T wieder als T' bezeichnet. Es wird nun gezeigt, dass jede beliebige affin lineare bijektive Abbildung T durch Multiplikation mit einer weiteren solchen Abbildung A in T' überführt werden kann. Da A ebenfalls eine bijektive Abbildung ist, gilt

$$A(\mathbb{F}^n) = \mathbb{F}^n. \quad (5.16)$$

Es wurde immer der gesamte Klartextrraum betrachtet. Da dieser von A bijektiv auf sich selbst abgebildet wird, bleiben die Aussagen des letzten Abschnitts für beliebiges T erhalten. Daraus folgt dann die Behauptung.

Existenz von T'

Es soll der folgende Zusammenhang erreicht werden:

$$(Z \circ T') \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} z_{11} & \cdots & z_{1r} & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ z_{r1} & \cdots & z_{rr} & 0 & \cdots & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} z_{10} \\ \vdots \\ z_{r0} \end{pmatrix}, \quad (5.17)$$

wobei die Einträge z_{ij} , $i, j = 1, \dots, r$, die entsprechenden Koeffizienten der affinen Funktionen z_1, \dots, z_r bezüglich des Urbilds $T'(x_1, \dots, x_n)$ darstellen. Die Matrix auf der rechten Seite ist dabei wieder eine $(r \times n)$ -Matrix, wobei die letzten $n - r$ Spalten Null sind. Für die weitere Argumentation werden folgende Notationen verwendet:

$$\begin{aligned} Z(x) &= M_Z x + v_Z, \\ T'(x) &= M_{T'} x + v_{T'}, \quad x \in \mathbb{F}^n. \end{aligned}$$

Damit lässt sich (5.17) wie folgt schreiben:

$$\begin{aligned}(Z \circ T')(x) &= M_Z(M_{T'}x + v_{T'}) + v_Z \\ &= M_Z M_{T'}x + M_Z v_{T'} + v_Z.\end{aligned}$$

Die i -te Spalte der Matrix auf der rechten Seite in (5.17) entsteht also gerade durch die Linksmultiplikation der i -ten Spalte der Matrix $M_{T'}$ mit M_Z , wobei $i = 1, \dots, n$. Um für die rechte Seite nun ein Ergebnis wie oben zu erzeugen, wo also die letzten $n - r$ Spalten Null sind, müssen folglich in $M_{T'}$ die letzten $n - r$ Spalten der Matrix bei Linksmultiplikation mit M_Z Null ergeben. Das bedeutet aber, dass diese Spalten im Kern von M_Z enthalten sind. Da Z nach Definition invertierbar ist und somit M_Z vollen Rang r hat, gilt für die Dimension des Kerns von M_Z nach dem Dimensionssatz

$$\dim(\ker M_Z) = n - r. \quad (5.18)$$

Die Matrix $M_{T'}$ der Abbildung T' ist ebenfalls nach Definition invertierbar, das heißt, die Spalten müssen linear unabhängig sein. Um obiges Ergebnis zu erzielen, werden für $M_{T'}$ $n - r$ Spaltenvektoren aus dem Kern von M_Z benötigt, die aber zusätzlich alle linear unabhängig sein müssen, damit T' invertierbar bleibt. Aussage (5.18) liefert hierfür aber nun gerade die erforderliche Voraussetzung. Es existieren demnach tatsächlich $n - r$ linear unabhängige Vektoren aus dem Kern von M_Z . Werden diese Vektoren als die $n - r$ letzten Spalten der Matrix $M_{T'}$ verwendet und die ersten r Spalten durch beliebige linear unabhängige Vektoren aus \mathbb{F}^n aufgefüllt, so entsteht eine Matrix, die genau die erforderlichen Bedingungen erfüllt. Der affine Teil $v_{T'}$ der Abbildung $T' = M_{T'} + v_{T'}$ kann beliebig gewählt werden, da er auf die obige Argumentation keinen Einfluss nimmt. Damit ist die Existenz einer Abbildung T' mit den gewünschten Eigenschaften allgemein gezeigt.

Überführung auf allgemeine T

Es ist also gezeigt, dass für jedes Perturbed Matsumoto Imai System zur Abbildung Z eine derartige Abbildung T' existiert, so dass die Störpolynome nur noch Funktionen in x_1, \dots, x_r sind. Damit ist also die Argumentation aus dem obigen Abschnitt 5.4.2 immer möglich. Nun kann aber eine allgemein gewählte invertierbare affin lineare Abbildung T immer durch eine weitere invertierbare affin lineare Abbildung A in T' überführt werden. Denn da die invertierbaren affin linearen Abbildungen eine Gruppe G bilden, gilt für jedes $T \in G$

$$\exists A \in G \text{ mit } T' = E \circ T' = T \circ \underbrace{T^{-1} \circ T'}_{=: A} = T \circ A \quad (5.19)$$

Dabei ist E das neutrale Element der Gruppe G . Mit (5.19) folgt daher, dass für jede mögliche Abbildung T eines beliebigen Perturbed Matsumoto Imai Systems immer eine Abbildung A gefunden werden kann, die T bijektiv derart abbildet, dass die Störpolynome wieder eine Funktion in x_1, \dots, x_r darstellen. Nach (5.16) gilt aber, dass die Abbildung A den Klartextrraum in sich selbst abbildet. Die Aussage des Abschnitts 5.4.2 kann somit verallgemeinert werden auf alle invertierbaren affin linearen Abbildungen T .

5.4.5 Abschätzung der Anzahl a nötiger +-Polynome

Der betrachtete Fall $\gcd(\lambda, n) = 1$

Das Hinzufügen der +-Polynome hat zur Folge, dass bei entsprechender Anzahl a von +-Polynomen der Defekt der Matrix $M_{x,a}$ für nahezu alle $x \in \mathbb{F}^n$ auf den gleichen Wert 1 verringert wird. Das bedeutet, dass der Testalgorithmus T fast immer den gleichen Wert ausgibt. Gemäß Abschnitt 4.4 bedeutet dies im Fall $\gcd(\lambda, n) = 1$, dass T meistens Null ausgibt und somit $\alpha = \Pr[T(x) = 0]$ sehr groß ist. In diesem Fall ist das Ziel also, dass $\alpha \approx 1$. Nun stellt der erste Eintrag im Vektor $\pi_0 \mathcal{P}_r^{r+a}$ gerade die Wahrscheinlichkeit für den Zustand mit Defekt 1 dar (vgl. Abschnitt 5.4.3). Also entspricht dieser erste Eintrag gerade α . Nähere Analysen von Ding und Gower in [DG05] zeigen, dass beispielsweise für ein System mit den Parametern $n = 136$, $r = 6$ und $\gcd(\lambda, n) = 1$ ein Wert von nur $a \geq 10$ ausreicht, um $\alpha > 0,998962$ zu erreichen. Für Systeme mit deutlich abweichenden Parametern kann α entsprechend mit Hilfe der Wahrscheinlichkeitsverteilung berechnet werden und ein geeigneter Wert für die Anzahl a der benötigten +-Polynome abgeschätzt werden.

Verallgemeinerung auf den Fall $\gcd(\lambda, n) \neq 1$

Bisher wurde der Fall $\gcd(\lambda, n) = 1$ untersucht (vgl. (5.7)). Dieser soll nun auf die übrigen Fälle $\gcd(\lambda, n) \neq 1$ ausgeweitet werden. Sei also

$$g := \gcd(\lambda, n).$$

Der Defekt der Matrix $M_{x,0}$ entspricht nach Satz 4.3.2 gerade dem Defekt der Matrix \mathcal{M}_x des entsprechenden C^* -Systems. Für deren Defekt gilt nun also $\text{defekt}(\mathcal{M}_x) = g$. Betrachtet man nun wieder wie oben allgemein eine Störung in r Spalten dieser Matrix, so können diese r veränderten Spalten unterschiedliche Auswirkungen haben. Dazu wird wieder in zwei Schritten vorgegangen. Zunächst werden r Spalten entfernt. Dadurch kann der Defekt der Matrix maximal um r auf $g + r$ ansteigen, falls r linear unabhängige Spalten entfernt wurden. Durch das anschließende Hinzufügen von r zufälligen Spalten kann der Defekt dann wieder um bis zu r sinken, falls alle neuen Spalten linear unabhängig sind. Falls aber im ersten Schritt r linear abhängige Spalten entfernt wurden, was im Fall $g > r$ möglich ist, dann steigt der Defekt durch das Entfernen der Spalten nicht an und bleibt auf dem Wert g . Im zweiten Schritt kann er dann aber natürlich dennoch wieder um r absinken, falls die neuen Spalten linear unabhängig sind. Zusammengefasst bedeutet dies für den Defekt der Matrix $M_{x,0}$ für beliebige x

$$\text{defekt}(M_{x,0}) \in \{g - r, \dots, g + r\}.$$

Um also vom allgemeinen Fall $\gcd(\lambda, n) = g$ ausgehend eine dem Fall $g = 1$ ähnliche Situation zu erhalten, müssen ungefähr g zusätzliche +-Polynome hinzugefügt werden. Somit kann dann der Defekt auf vergleichbar niedrige Werte bis hin zum Wert 1 verringert werden.

5.4.6 Analyse der Auswirkungen der +-Modifikation

Basierend auf den Erkenntnissen der letzten Abschnitte kann nun mit Hilfe der aus dem Markov-Modell gewonnenen Wahrscheinlichkeitsverteilung analysiert werden, welche Auswirkungen eine bestimmte Anzahl a an +-Polynomen

auf den Defekt der Matrix $M_{x,a}$ hat. Ding und Gower konnten die mit dem Markov-Modell errechneten Daten auch experimentell verifizieren. Diese experimentell gewonnenen Daten werden hier aus Gründen der Übersichtlichkeit nicht vorgestellt, für nähere Details sei auf [DG05] verwiesen. Als Beispiel wurde unter anderem ein Perturbed Matsumoto Imai System mit den Parametern $q = 2$, $n = 36$, $r = 6$ und $\lambda = 4$ getestet. Dabei wurde für $2^{15} = 32768$ Vektoren x aus dem Klartextraum geprüft, welchen Defekt sie für die Matrix $M_{x,a}$ zur Folge haben. Es wurden +-Modifikationen mit $a = 1, \dots, 11$ +-Polynomen untersucht. In Tabelle 5.1 ist für jeden auftretenden Defekt δ jeweils die Anzahl $n_{\delta,a}$ der Vektoren, die zum entsprechenden Defekt führten, notiert.

a	$x \notin \mathcal{K}$					$x \in \mathcal{K}$			
	$\delta = 1$	$\delta = 2$	$\delta = 3$	$\delta = 4$	$\delta = 5$	$\delta = 1$	$\delta = 2$	$\delta = 3$	$\delta = 4$
0	101	2274	16272	1865	37	0	0	0	492
1	22073	9428	758	17	0	0	0	430	62
2	26750	5316	205	4	0	0	325	160	7
3	29376	2841	58	1	0	161	285	46	1
4	30799	1462	14	0	0	304	176	13	0
5	31538	735	2	0	0	385	103	4	0
6	31897	379	0	0	0	436	55	1	0
7	32096	180	0	0	0	462	30	0	0
8	32186	90	0	0	0	475	16	0	0
9	32240	36	0	0	0	480	11	0	0
10	32261	15	0	0	0	486	6	0	0
11	32267	9	0	0	0	490	2	0	0

Tabelle 5.1: Nach dem Markov-Modell berechnete Werte für $n_{\delta,a}$ für ein System mit dem Parametern $(q, n, r, \lambda) = (2, 36, 6, 4)$ bei 2^{15} überprüften Vektoren

Interpretation der Ergebnisse

Für das untersuchte System gilt $\gcd(\lambda, n) = \gcd(4, 36) = 4$. Für den klassischen Fall des Perturbed Matsumoto Imai Systems ohne hinzugefügte +-Polynome, also $a = 0$, gilt demnach, dass für alle $x \in \mathcal{K}$ der Defekt $\delta = 4$ verursacht wird. Die Einträge in den anderen Spalten sind daher Null. Für $x \notin \mathcal{K}$ hingegen werden unterschiedliche Defekte verursacht, die meisten Vektoren verursachen einen Defekt $\delta \neq 4$. Mit zunehmendem a , also zunehmender Anzahl hinzugefügter +-Polynome ändert sich diese Situation jedoch: Bei $a = 11$ +-Polynomen ist ein Zustand erreicht, in dem sowohl nahezu alle $x \in \mathcal{K}$ als auch nahezu alle $x \notin \mathcal{K}$ den Defekt $\delta = 1$ verursachen. Der Testalgorithmus T könnte somit unmöglich eine Entscheidung treffen, ob ein Vektor x in \mathcal{K} enthalten ist oder nicht. Die Rekonstruktion von \mathcal{K} wäre somit nicht möglich und ein differentieller Angriff erfolglos. Das Hinzufügen von 11 +-Polynomen hat das Perturbed Matsumoto Imai System also erfolgreich gegen einen differentiellen Angriff abgesichert.

5.5 Empfohlene Parameter

Ding und Gower schlagen in [DG05] ein PMI+ System mit den Parametern $n = 84$, $q = 2$, $r = 6$ und $\lambda = 4$ sowie $a = 14$ zusätzlichen +-Polynomen oder alternativ ein System mit $n = 136$, $q = 2$, $r = 6$, $\lambda = 8$ und $a = 18$ zusätzlichen +-Polynomen als sichere Systeme vor. Sie erreichen einen Sicherheitslevel von 2^{80} . Generell gilt, dass die Anzahl der +-Polynome nicht zu groß werden sollte, da dadurch ein Angriff des Systems mit Hilfe von Gröbner Basen begünstigt werden kann (vgl. [CKPS, YCC04]). Aus dem selben Grund sollte daher $g = \gcd(\lambda, n)$ nicht zu groß sein, da damit die Anzahl der benötigten +-Polynome noch größer würde. Ding und Gower empfehlen daher als allgemeine Richtlinien $n > 83$, $r = 6$ bei $a = 14$ +-Polynomen, solange $g \leq 4$.

5.6 Die Größe der Schlüssel

Im Folgenden wird der Speicherbedarf für die Schlüssel eines PMI+-Systems analysiert. Es wird dabei ein System mit den oben genannten Parametern $n = 84$, $q = 2$, $\lambda = 4$, $r = 6$ und $a = 14$ betrachtet. Die Bestandteile der Schlüssel umfassen bis auf leichte Modifikationen die gleichen Komponenten wie bei der Perturbed Matsumoto Imai Chiffre (vgl. Abschnitt 3.3).

5.6.1 Größe des öffentlichen Schlüssels

Der öffentliche Schlüssel beinhaltet zunächst Angaben zum Grundkörper $\mathbb{F} = GF(q)$ mit q Elementen sowie der Nachrichtenlänge n . Diese Systemparameter haben einen sehr geringen Speicherbedarf und werden daher bei der weiteren Berechnung vernachlässigt. Sind bei einer Implementierung des Systems der Grundkörper und die Nachrichtenlänge fest vorgeschrieben, müssen sie überhaupt nicht gespeichert werden. Der öffentliche Schlüssel beinhaltet außerdem das MQ -System \hat{P}^+ , also ein System von $n + a$ quadratischen Polynomen über \mathbb{F} in den Variablen x_1, \dots, x_n von der folgenden Form (vgl. Definition 1.2.1):

$$\sum_{1 \leq j \leq k \leq n} \gamma_{i,jk} x_j x_k + \sum_{1 \leq j \leq n} \beta_{i,j} x_j + \alpha_i, \quad i = 1, \dots, n + a. \quad (5.20)$$

Eine Zeile dieses Systems enthält im allgemeinen Fall $n^2 + n + 1$ Terme und entsprechend viele Koeffizienten. Diese müssen alle gespeichert werden, da die Polynome bei PMI+ keine spezielle Form haben, die einige Koeffizienten überflüssig machen könnte. Somit entsteht ein Speicherbedarf von

$$(n + a)(n^2 + n + 1)$$

Koeffizienten aus \mathbb{F} . Jeder Koeffizient benötigt 1 Bit Speicherplatz, da $q = 2$. Damit summiert sich der Speicherbedarf für das gesamte System auf 699818 Bits. Die Größe des öffentlichen Schlüssels beträgt somit ungefähr 700 Kbit bzw. 88 KByte.

5.6.2 Größe des privaten Schlüssels

Der private Schlüssel umfasst ebenso wie der öffentliche Angaben zum Grundkörper \mathbb{F} und der Nachrichtenlänge n , diese Systemparameter werden jedoch

aus den oben genannten Gründen vernachlässigt. Darüber hinaus enthält der private Schlüssel die beiden affin linearen Abbildungen S^+ und T . S^+ besteht aus einer $(n + a) \times (n + a)$ -Matrix und einem Vektor mit $n + a$ Komponenten aus \mathbb{F} , es müssen also

$$(n + a)^2 + n + a$$

Werte gespeichert werden. Die Abbildung T umfasst entsprechend

$$n^2 + n$$

Komponenten. Des Weiteren enthält der private Schlüssel die affin lineare Abbildung Z und die Störungsmenge M_p bzw. das Polynom p . Allerdings bedarf p im Allgemeinen weniger Speicherplatz als M_p , daher wird der Speicherplatz für p betrachtet. Z besteht aus einer $(r \times n)$ -Matrix und einem Vektor mit r Komponenten, es müssen also

$$rn + r$$

Werte aus \mathbb{F} gespeichert werden. p ist ein System von n quadratischen Polynomen in den Variablen z_1, \dots, z_r . Ein Vergleich mit (5.20) zeigt, dass für p

$$n(r^2 + r + 1)$$

Koeffizienten aus \mathbb{F} gespeichert werden müssen. Schließlich wird noch das geheime Polynom P^* benötigt. Hier muss, da die Form des Monoms bekannt ist, nur noch der Parameter λ gespeichert werden. Außerdem sollte der Wert a der Anzahl der $+$ -Polynome gespeichert werden. Diese Werte sind allerdings in ihrem Speicherbedarf vernachlässigbar, so dass sie in der Rechnung nicht berücksichtigt werden. Das gleiche gilt für die Koeffizienten des irreduziblen univariaten Polynoms u , das für die Darstellung des Erweiterungskörpers \mathbb{E} benötigt wird. Denn der Grad dieses Polynoms entspricht dem Grad der Körpererweiterung, also n . Somit ist der Speicherbedarf für diese Koeffizienten ebenfalls vernachlässigbar. Damit summiert sich die Anzahl an zu speichernden Koeffizienten aus \mathbb{F} auf

$$(n + a)^2 + n + a + n^2 + n + rn + r + n(r^2 + r + 1).$$

Der Speicherbedarf beträgt somit 20964 Bits. Der private Schlüssel benötigt also einen Speicherplatz von ungefähr 21 KBit bzw. 2,6 KByte.

5.7 Fazit

Die PMI+ Chiffre stellt eine Modifikation dar, die in bemerkenswert einfacher Weise eine doch verhängnisvolle Schwachstelle der Perturbed Matsumoto Imai Chiffre sehr gezielt behebt. Zum einen ist das System wirkungsvoll gegen differentielle Angriffe geschützt und erreicht somit nach derzeitigen Erkenntnissen ein sehr hohes Sicherheitsniveau. Zum anderen ist die Modifikation dabei aber sehr übersichtlich und einfach aufgebaut. Schon eine sehr geringe Zahl an $+$ -Polynomen reicht aus, um einen wirkungsvollen Effekt zu erzielen. Dadurch wird die Effizienz des System durch die Modifikation kaum beeinträchtigt. Tatsächlich hat eine zu hohe Anzahl von $+$ -Polynomen, wie bereits erwähnt, sogar den kritischen Effekt, den Angriff des Systems mit Gröbner Basen zu begünstigen. Die oben beschriebene Tatsache, dass die $+$ -Modifikation sogar dazu dienlich

sein kann, den korrekten Klartext bei der Entschlüsselung zu identifizieren, verbessert die Effizienz gegenüber dem Perturbed Matsumoto Imai System sogar geringfügig, da keine zusätzlichen Schritte notwendig werden. Darüber hinaus greift die Modifikation, da es sich um eine externe Störung handelt, nicht so tief in das System ein, wie es beispielsweise die interne Störung bei der Perturbed Matsumoto Imai Modifikation tut. Im letzteren Fall sind das zugrunde liegende System und die modifizierenden Elemente nahezu untrennbar miteinander verwoben. Dadurch entstehen unter Umständen nicht vorhersehbare neue Effekte, die sich für Angriffe nutzen lassen. Genau dies ist bei der Perturbed Matsumoto Imai Chiffre geschehen und hat den differentiellen Angriff ermöglicht. Da die +-Modifikation bei PMI+ transparenter verläuft und vom zugrunde liegenden System stärker entkoppelt ist, sind hier weniger neue Effekte zu erwarten, was die Sicherheitsanalyse des Systems vereinfacht und einen neuen Angriff unwahrscheinlicher macht. Allerdings besteht natürlich durch die stärkere Trennung von Basis-System und Modifikation die Idee, die beiden Teile durch einen geeigneten Angriff wieder voneinander zu trennen und das System auf diesem Weg zu brechen. Jedoch wird die Gefahr eines solchen Angriffs von Ding und Gower als gering eingeschätzt, da kein geeignetes Mittel zur Verfügung steht, um die +-Polynome von den Polynomen des zugrunde liegenden Perturbed Matsumoto Imai Systems zu unterscheiden.

Zusammengefasst lässt sich sagen, dass PMI+ ein Kryptosystem darstellt, das den Ansatz eines Public Key Kryptosystems auf Basis des C^* -Systems nach gegenwärtigem Kenntnisstand auf einem sehr hohen Sicherheitslevel umsetzt.

Literaturverzeichnis

- [Art98] Michael Artin: *Algebra*, Birkhäuser Verlag, 1998
- [Bol01] Béla Bollobás: *Random Graphs*, Cambridge University Press, Second Edition, 2001
- [BS96] E. Bach and J. Shallit: *Algorithmic Number Theory*, MIT Press, Volume 1 - Efficient Algorithms, 1996
- [Buc03] Johannes Buchmann: *Einführung in die Kryptographie*, Springer Verlag, 2003
- [CKPS] Nicolas Courtois, Alexander Klimov, Jacques Patarin und Adi Shamir: *Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations*, Eurocrypt 2000, LNCS 1807, S. 392-407
- [DG05] Jintai Ding und Jason E. Gower: *Inoculating Multivariate Schemes Against Differential Attacks*, Cryptology ePrint Archive, Report 2005/255, 2005
- [Din04] Jintai Ding: *A New Variant of the Matsumoto-Imai Cryptosystem through Perturbation*, PKC 2004, LNCS 2947, S. 305-318, Springer Verlag, 2004
- [FGS05] Pierre-Alain Fouque, Louis Granboulan und Jacques Stern: *Differential Cryptanalysis for Multivariate Schemes*, Eurocrypt 2005, LNCS 3494, S. 341-353, 2005
- [MI88] Hideki Imai, Tsutomu Matsumoto: *Public Quadratic Polynomial-Tuples for Efficient Signature-Verification and Message-Encryption*, Eurocrypt 1988, Springer Verlag, S. 419-453
- [Pat95] Jacques Patarin: *Cryptanalysis of the Matsumoto and Imai Public Key Scheme of Eurocrypt '88*, Advances in Cryptology - CRYPTO '95, Springer Verlag, S. 248-261, 1995
- [WP05] Christopher Wolf und Bart Preneel: *Taxonomy of Public Key Schemes based on the problem of Multivariate Quadratic equations*, Cryptology ePrint Archive, Report 2005/077, 2005
- [YCC04] Bo-Yin Yang, Jiun-Ming Chen und Nicolas Courtois: *On Asymptotic Security Estimates in XL and Gröbner Bases-Related Algebraic Cryptanalysis*, ICICS 2004, LNCS 3269, S. 410-413