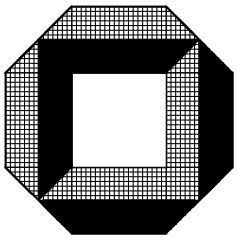
Seminar

Kryptographie und Mathematik



Universität Karlsruhe (TH)
Fakultät für Informatik
Institut für Algorithmen und Kognitive Systeme

Prof. Dr. Th. Beth
Dr. W. Geiselmann
Dipl.-Inform. B. Grohmann
Dr. R. Steinwandt
Dipl.-Inform. P. Wocjan

Wintersemester 2000/2001

Inhaltsverzeichnis

Vortrag 1

Hidden Monomial Cryptosystems

Frank-Michael Krupp

1.1 Einleitung

Ein Public-Key-Verfahren nutzt die Eigenschaft, dass es mathematische Operationen gibt, die in der einen Richtung (verschlüsseln) schnell berechenbar sind, jedoch in der Rückrichtung (entschlüsseln) nur bei Kenntnis geheimer Parameter (secret key) mit aktzeptablem Aufwand handhabbar sind. Bisher sind vor allem zwei Verfahren bekannt, die die obigen Eigenschaften erfüllen: das Faktorisieren von großen Zahlen, wie es zum Beispiel bei RSA angewendet wird, und das diskrete Logarithmus-Problem, das bei ElGamal und Diffie-Hellman verwendet wird.
Eine relativ neue, weitere Möglichkeit ergibt sich durch Ausnutzen der Schwierigkeit des Lösens nichtlinearer Gleichungssysteme über endlichen Körpern. Das erste Verfahren dieser Art entwickelten 1988 T. Matsumoto und H. Imai [2]. Es wird im ersten Teil dieses Textes analysiert. Ein weiteres Verfahren aus dieser Klasse der „Hidden Monomial Cryptosystems“ stellte J. Patarin 1995 vor [3], nachdem er eine Angriffsmöglichkeit für das Imai-Matsumoto-System gefunden hatte [4]. Aber auch Patarins „Little Dragon“ ist unsicher [3]. Das System und die Kryptanalyse werden im zweiten Teil dieses Referats behandelt. Der Vorteil von „Hidden Monomial Systems“ ist zum einen die geringe Expansionsrate, eine verschlüsselte Datei bleibt klein, zum anderen sind die Verfahren schnell und einfach in Hardware zu implementieren [5]. Geschwindigkeit ist bei Public-Key-Verfahren, die um den Faktor 100 langsamer als symmetrische Verfahren sind, ein wichtiges Merkmal. Dementsprechend entwickelten sich weitere Verfahren, unter anderem „Big Dragon“ und „Double-Round Quadratic Enciphering“ [6], die sich bisher resistent gegen alle Angriffsbemühungen gezeigt haben, allerdings erst wenige Jahre alt sind und noch nicht ausgiebig genug überprüft wurden, um als sicher zu gelten.

1.2 Das Imai-Matsumoto-System

1.2.1 Notation

Gegeben ist ein endlicher Grundkörper $\mathbb{F}_q$, wobei q eine Zweierpotenz ist.
$\mathbb{K}$ ist ein Erweiterungskörper von $\mathbb{F}_q$, also insbesondere ein $\mathbb{F}_q$-Vektorraum, der von der Basis $(\beta_1, \ldots, \beta_n)$ aufgespannt wird.
$\vec{x} = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$ ist der Klartextvektor,
$\vec{y} = (y_1, \ldots, y_n) \in \mathbb{F}_q^n$ ist das Chiffrat,
$\vec{u} = (u_1, \ldots, u_n) \in \mathbb{F}_q^n$, $\vec{v} = (v_1, \ldots, v_n) \in \mathbb{F}_q^n$ werden als Hilfsvektoren benötigt.
Zu jedem Vektor $\vec{u} \in \mathbb{F}_q^n$ existiert das zugehörige Körperelement (fettgedruckt) $\mathbf{u} = u_1 \cdot \beta_1 + \ldots + u_n \cdot \beta_n \in \mathbb{K}$.

1.2.2 Überblick

Der Kern des Verfahrens ist die mononomiale Abbildung $\mathbf{u} \mapsto \mathbf{u}^h$. Da diese Abbildung invertierbar sein sollte, damit auch wieder entschlüsselt werden kann, sind an h einige Bedingungen zu stellen. Dies führt dazu, dass die Zahl der möglichen h nicht groß genug ist (im $\mathbb{F}_q^n$ weniger als n), um gegen Rateversuche eines Angreifers sicher zu sein. Deshalb wird die mononomiale Abbildung durch den Einsatz von zwei affinen Transformationen verschleiert („Hidden Monomial“). Wenn man einige Körpereigenschaften ausnutzt, ist es möglich, die langsame Exponentiation durch lineare Transformationen zu ersetzen und damit ein Gleichungssystem zu erhalten, in dem man nicht die geheimen Werte ablesen kann. Man erhält ein nichtlineares Gleichungssystem in $\vec{x}$, das zusammen mit q den öffentlichen Schlüssel darstellt.

Klartext $\vec{x} = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$				Chiffrat $\vec{y} = (y_1, \ldots, y_n) \in \mathbb{F}_q^n$
$\Downarrow$				$\Downarrow$
$\vec{u} = A\vec{x} + \vec{c}$	$\Rightarrow$	$\mathbf{v} = \mathbf{u}^h$	$\Rightarrow$	$\vec{y} = B^{-1}(\vec{v} - \vec{d})$

Geheime Parameter

invertierbare $n \times n$-Matrizen A, B	konstante Vektoren $\vec{c}, \vec{d}$
Basis $(\beta_1, \ldots, \beta_n)$	Exponent h

1.2.3 Verschlüsseln und Entschlüsseln

Im Zentrum des Verfahrens steht die invertierbare Abbildung $\mathbf{u} \mapsto \mathbf{u}^h$ mit $0 < h < q^n$ und $h = q^\theta + 1$. Von h wird gefordert, dass $ggT(h, q^n - 1) = 1$ gilt. Denn für die Rückrichtung benötigt man ein zu h inverses Element h'. Mit dem erweiterten euklidschen Algorithmus ist genau diese Eigenschaft erfüllt, da gilt: $\exists h', \exists a$ mit $h'h + a \cdot (q^n - 1) = 1 \Rightarrow h'$ ist das multiplikative Inverse von h mod $q^n - 1$.
Nebenbemerkung: Aus dieser ggT-Bedingung folgt, dass q gerade sein muß, ansonsten läßt sich kein geeignetes h finden, denn für alle h gilt dann: $ggT(h, q^n - 1) > 1$. Die anfangs erwähnte Eigenschaft, dass q eine Zweierpotenz sein soll, wird für Behauptung 1 benötigt.
Die Werte h und h' bleiben geheim, sind aber leicht zu erraten, da es wegen der Bedingung $0 < h < q^n$ weniger als n Wahlmöglichkeiten gibt. Zusätzlich gibt es deshalb zwei geheime affine Transformationen. Dazu benötigt man die geheim zu haltenden invertierbaren $n \times n$-Matrizen A und B und die konstante Vektoren $\vec{c}$ und $\vec{d}$. Der Klartext $\vec{x}$ wird in den Hilfsvektor $\vec{u}$ transformiert $\vec{u} = A\vec{x} + \vec{c}$. Dann wird $\vec{u}$ mit der Basis $\vec{\beta}$ als Körperelement $\mathbf{u} = u_1 \cdot \beta_1 + \ldots + u_n \cdot \beta_n$ dargestellt. Die oben erwähnte anschließende Exponentiation $\mathbf{v} = \mathbf{u}^h = \mathbf{u}^{q^\theta}\mathbf{u}$ kann wie folgt durch *lineare* Transformationen erfolgen.
Behauptung 1 $(a + b)^q = a^q + b^q$ in $\mathbb{F}_q$
Mit der binomischen Formel gilt:

$$(a+b)^q = a^q + b^q + \underbrace{\sum_{i=1}^{q-1} \frac{q!}{i!(q-i)!} a^i b^{q-i}}_{=0}$$

Die gemischten Terme fallen weg, da sie ein Vielfaches von q sind. ■
Die Behauptung gilt auch für Exponenten der Form q^θ (einfacher Induktionsbeweis). Ebenso läßt sich die Behauptung auf Summen mit mehr als zwei Summanden übertragen (wiederum einfacher Induktionsbeweis). Insgesamt hat man nun $\left(\sum_{i=1}^{n} a_i\right)^{q^\theta} = \sum_{i=1}^{n} a_i^{q^\theta}$.
Mit der nächsten Behauptung wird die Vereinfachung der Summanden ermöglicht.
Behauptung 2 $(u_i\beta_i)^{q^\theta} = u_i\beta_i^{q^\theta}$
O.B.d.A. sei $\theta = 1$. Zu zeigen ist $u^q = u$. Die multiplikative Gruppe des endlichen Körpers $\mathbb{F}_q$ hat Gruppenordnung ord$=q-1$, also $q-1$ Elemente. Aus der linearen Algebra ist bekannt, dass gilt $u^{ord} = 1$ (Neutralelement bei Multiplikation). Also ist $u^q = u^{q-1}u = u^{ord}u = 1u$. ■
Die nächste Behauptung führt auf eine einfachere Darstellung:
Behauptung 3 $\beta_i^{q^\theta} = \sum_{j=1}^{n} p_{ij}^{(\theta)} \beta_j$ und $\beta_j\beta_k = \sum_{l=1}^{n} m_{jkl}\beta_l$
Dies ist eine Darstellung bezüglich der ursprünglichen Basis $\{\beta_1, \ldots, \beta_n\}$. ■
Damit kann man folgern:

$$\begin{aligned}
\sum_{i=1}^{n} v_i\beta_i = \mathbf{v} = \mathbf{u}^{q^\theta}\mathbf{u} &= \left(\sum_{i=1}^{n} u_i\beta_i\right)^{q^\theta} \left(\sum_{k=1}^{n} u_k\beta_k\right) \\
&= \left(\sum_{1\le i,j\le n} p_{ij}^{(\theta)} u_i\beta_j\right) \left(\sum_{k=1}^{n} u_k\beta_k\right) \\
&= \sum_{1\le i,j,k,l\le n} p_{ij}^{(\theta)} u_i u_k m_{jkl}\beta_l
\end{aligned}$$

Schließlich werden die beiden Transformationsgleichungen

$$u_i = \sum_{l=1}^{n} a_{il}x_l + c_i; \quad v_i = \sum_{l=1}^{n} b_{il}y_l + d_i$$

benötigt, man kann nach y_i auflösen, da die Matrizen regulär sind und erhält:

$$\begin{aligned} y_1 &= \sum_{i,j} c_{ij}^{(1)} x_i x_j + \sum_k c_k^{(1)} x_k + c^{(1)} \\ &\vdots \\ y_n &= \sum_{i,j} c_{ij}^{(n)} x_i x_j + \sum_k c_k^{(n)} x_k + c^{(n)} \end{aligned}$$

Das sind n Gleichungen von Polynomen des Grades 2 in $x_1, \ldots, x_n$. Diese n Gleichungen werden zusammen mit q veröffentlicht. Will jemand eine Nachricht schicken, so setzt er seinen Klartext $x_1, \ldots, x_n$ ein und erhält sofort das Chiffrat $y_1, \ldots, y_n$. Der Besitzer der geheimen Informationen $A, B, \vec{c}, \vec{d}, \vec{\beta}, (h, h')$ kann den Klartext erhalten, indem er die Umformungen rückgängig macht. Er braucht B und $\vec{d}$, um die zweite affine Transformation zu invertieren, dann die Basis $\vec{\beta}$ um das korrespondierende Körperelement $\mathbf{v}$ zu bekommen, mit h' wird die Exponentiation umgekehrt, und das erhaltene $\mathbf{u}$ wird — nachdem es mit $\vec{\beta}$ in den Vektor $\vec{u}$ umgewandelt wurde — mit A und $\vec{c}$ in den Klartext $\vec{x}$ transformiert. Ein Angreifer steht zunächst vor einem nichtlinearen Gleichungssystem. Mit einem Umformungstrick, der in 1.2.5 dargestellt wird, kann er daraus ein lineares Gleichungssystem gewinnen. Bevor auf den Angriff näher eingegangen wird, folgt ein kleines Beispiel, das den Ablauf des Verfahrens erläutern soll.

1.2.4 Beispiel

Damit das Beispiel übersichtlich bleibt, werden kleine Werte gewählt. Als Zweierpotenz wird $q = 2$ gesetzt. Der Körper $\mathbb{K}$ soll vom Grad $n = 3$ sein. $\mathbb{K}$ ist gegeben durch die Menge der Polynome über dem Grundkörper $\mathbb{F}_2$ modulo $f(X) = X^3+X+1$. Als einfache Basis bietet sich $\{\beta_1, \beta_2, \beta_3\} = \{1, X, X^2\}$ an. Ein h, das die Bedingung ggT$(h, 2^3 - 1)$=1 erfüllt, ist beispielsweise $h = 3$, damit ist $h' = 5$ und $\theta = 1$. Die affinen Transformationen können folgende Werte aufweisen:

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} \; A^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} \; B = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \; B^{-1} = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \; \vec{c} = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \; \vec{d} = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$$

Die erste affine Transformation $\vec{u} = A \cdot \vec{x} + \vec{c}$ führt auf $u_1 = x_1 + 1$, $u_2 = x_2 + x_3$, $u_3 = x_1 + x_3 + 1$. Die Exponentiation wird in diesem Beispiel direkt ausgerechnet, da es bei diesen kleinen Zahlen schneller auf direktem Wege geht: $\mathbf{v} = \mathbf{u}^3 = \mathbf{u}^2\mathbf{u} = (u_1\beta_1^2 + u_2\beta_2^2 + u_3\beta_3^2)(u_1\beta_1 + u_2\beta_2 + u_3\beta_3) = (u_1 + u_2x^2 + u_3x^4)(u_1 + u_2X + u_3X^2)$ Ausmultipliziert und modulo $f(X)$ gerechnet ergibt:

$$\begin{aligned} v_1 &= x_2^2 + x_1x_2 + x_1x_3 + x_2x_3 + x_3^2 + x_2 + x_3 \\ v_2 &= x_1x_2 + x_2 + x_1^2 + 1 + x_2^2 + x_2 + x_3^2 \\ v_3 &= x_1x_2 + x_1x_3 + x_2 + x_3 + x_1^2 + x_3^2 + 1 \end{aligned}$$

Noch eine letzte affine Transformation $\vec{y} = B^{-1}(\vec{v} - \vec{d})$ und es können Gleichungen veröffentlicht werden:

$$\begin{aligned} y_1 &= x_1^2 + x_2^2 + x_2x_3 \\ y_2 &= x_1^2 + x_1x_3 + x_2x_3 + x_3 \\ y_3 &= x_1x_2 + x_1x_3 + x_2 + x_3 + x_1^2 + x_3^2 \\ q &= 2 \end{aligned}$$

Um die geheime Nachricht 101... zu übermitteln, wird dieser Vektor $\vec{x}$ in die Gleichungen eingesetzt, und man erhält den Chiffratvektor $y_1 = 1$, $y_2 = 1$, $y_3 = 0$.
Der rechtmäßige Empfänger und damit Besitzer des secret keys $A, B, \vec{c}, \vec{d}, \vec{\beta}, (h, h')$ will die chiffrierte Nachricht lesen. Er rechnet $\vec{v} = B \cdot \vec{y} + \vec{d}$ und erhält $v_1 = 0$, $v_2 = 0$, $v_3 = 1$. Die Exponentiation $\mathbf{u} = \mathbf{v}^5 = (x^2)^5$ liefert $u_1 = 0$, $u_2 = 1$, $u_3 = 0$, und die affine Transformation $\vec{x} = A \cdot (\vec{u} - \vec{c})$ führt wieder zum Klartext $x_1 = 1, x_2 = 0, x_3 = 1$. Ein unrechtmäßiger Empfänger hat zunächst keine Chance, die Nachricht zu erfahren.

1.2.5 Kryptanalyse

1995 stellte J. Patarin auf der Crypto[4] einen Angriff auf das Imai-Matsumoto-System vor. Damit ist es möglich, die Größe des Suchraumes so stark zu reduzieren, dass das System ineffizient wird. Der Angriff erfolgt auf die Gleichung $\mathbf{v} = \mathbf{u}^h$ durch Potenzieren mit $q^\theta - 1$ und multiplizieren mit $\mathbf{uv}$.

$$(1) \quad \mathbf{uv}^{q^\theta} = \mathbf{u}^{q^{2\theta}}\mathbf{v}$$

Jetzt ist schon offensichtlich, wie der Angriff verläuft. Im Körper $\mathbb{F}_q$ ist eine Exponentiation mit q wiederum linear darstellbar. Analoge Umformungen wie beim Herleiten der öffentlichen Gleichungen führen auf

$$\sum_{1\le i,j,k,l\le n} p_{jk}^{(\theta)} u_i v_j m_{ikl} \beta_l = \sum_{1\le i,j,k,l\le n} p_{ik}^{(2\theta)} u_i v_j m_{kjl} \beta_l.$$

Einsetzen der affinen Transformationsgleichungen für u_i und v_i und Variablenumbenennung führen zu den folgenden $l = 1, \ldots, n$ Gleichungen:

$$(2) \quad \sum_{1\le i,j\le n} \alpha_{ijl} x_i y_j + \sum_{1\le i\le n} (\beta_{il} x_i + \gamma_{il} y_i) + \delta_l = 0$$

Da der Angreifer weder $\vec{u}, \vec{v}$ noch die affinen Transformationen $A, B, \vec{c}, \vec{d}$ oder Basis $\vec{\beta}$ kennt, sind alle Koeffizienten zunächst unbekannt. Es gibt zwei Faktoren, die den Angriff dennoch ermöglichen. Wie schon bemerkt, ist dieses Gleichungssystem *linear* in $\vec{x}$. Außerdem kann niemand daran gehindert werden, den öffentlichen Schlüssel zu verwenden, um eine große Anzahl Klartext/Schlüsseltext-Paare $(x_1, \ldots, x_n, y_1, \ldots, y_n)$, zu erzeugen. Diese kann man in das obige Gleichungssystem einsetzen und eine maximale Anzahl von L linear unabhängigen Gleichungen erhalten, welche jedoch nicht ausreichen, um alle Koeffizienten zu bestimmen, weil durch das Potenzieren mit $q^\theta - 1$ neue künstliche Lösungen entstanden sind. Beispielsweise hat die Gleichung $\sqrt{x} = -2$ erst nach dem Quadrieren $x = 4$ eine „Lösung“. Der Angreifer hört die Leitung ab und setzt den gefundenen verschlüsselten Text $\vec{y}_0$ in die L Gleichungen ein. Dabei kann es vorkommen, dass dadurch ein paar Gleichungen linear abhängig werden und wegfallen, es bleiben $M \le L$ Gleichungen. Natürlich erfüllt die ursprüngliche Nachricht $\vec{x}_0$ die Gleichungen. Insgesamt hat man q^{n-M} Lösungen, da es n Unbekannte $x_1, \ldots, x_n$ gibt, aber nur M Gleichungen, wobei jede Unbekannte q Werte annehmen kann (eleganter formuliert: der Lösungsraum ist ein affiner $(n-M)$-dim. Unterraum in $\mathbb{F}_q^n$). Als letzten Schritt in der Kryptanalyse fehlt nur noch eine gute Abschätzung für die Größe dieses Unterraums. Ist dieser sehr groß, dann ist der Angriff auf diese Weise unmöglich, ist er klein, dann hat der Angreifer gewonnen. Im Imai-Matsumoto-System tritt letzteres ein. Die Dimension des affinen Unterraums hat nur ein Drittel der Größe von $\mathbb{F}_q^n$. Das heißt, für die ursprünglich geplante Sicherheit muß nun ein weitaus größerer Aufwand eingeplant werden, damit ist das System ineffizient.
Kurze Beweisidee (für den vollständigen Beweis wird wieder auf [1] verwiesen): Man kann vereinfachend annehmen, dass eine Bijektion zwischen dem Lösungsraum von (1) und (2) besteht. Daher kann man zur Abschätzung der Lösungsanzahl die Gleichung (1) verwenden. Hält man $\mathbf{v}_0$, gegeben durch $\mathbf{y}_0$ fest, so kann man $\mathbf{v}_0^{q^\theta - 1} = \mathbf{u}_0^{h(q^\theta-1)}$ und $\mathbf{v}_0^{q^\theta-1} = \mathbf{u}^{h(q^\theta-1)}$ nach $\mathbf{u}$ auflösen: $\mathbf{u}_0^{q^\theta-1} = \mathbf{u}^{q^\theta-1}$ Das bedeutet, dass sich die Lösungen nur durch eine $(q^\theta-1)$te Einheitswurzel unterscheiden. Da die Ordnung der multiplikativen Gruppe von $\mathbb{K}$ $ord = q^n - 1$ beträgt, gibt es insgesamt $ggT(q^\theta - 1, ord)$ Einheitswurzeln. Weiter gilt $ggT(q^\theta - 1, ord) = q^d - 1$ mit $d = ggT(\theta, n)$. Mit der trivialen Null-Lösung sind es somit q^d mögliche Klartexte, die zum abgefangenen Chiffrat passen. Eine weitere Abschätzung führt auf $d \le n/3$, somit hat der Suchraum nur ein Drittel der ursprünglichen angenommenen Dimension.

1.3 Patarins Little Dragon

1.3.1 Vergleich zu Imai-Matsumoto

Nachdem das Imai-Matsumoto-System gebrochen wurde [4], veröffentlichte Patarin ein auf diesem aufbauendes System, dem er den Namen Little Dragon gab [3]. Es unterscheidet sich nur in der Wahl des Exponenten h, denn allein daran war zunächst das Imai-Matsumoto-System gescheitert. Jedoch haben Patarin und Coppersmith 1996 eine weitere Angriffsmöglichkeit entdeckt, die auch dieses System bricht [3]. Es soll diesmal für den Exponenten h gelten:

$$h = q^\theta + q^\varphi - 1 \qquad 0 < h < q^n$$

Außerdem erfüllt h wieder die Umkehrbarkeitsbedingung $ggT(h, q^n - 1) = 1$. Weitere einschränkende Bedingungen an h entfallen bei diesem System. Wiederum muß h verschleiert werden durch Transformationen, weil es weniger als n Belegungsmöglichkeiten gibt. Zur Vereinfachung des in Abschnitt 1.3.4 vorgestellten Angriffs, wird hier $\vec{c} = 0$ und $\vec{d} = 0$ angenommen (die Notation ist analog zum Imai-Matsumoto-System). Auch wenn man nicht lineare, sondern affine Transformationen ($\vec{c} \neq 0$, $\vec{d} \neq 0$) verwendet, bleibt der Angriff mit gleichem Aufwand erfolgreich. Der Initialisierungsprozess für die öffentlichen Gleichungen läuft wie bei Imai-Matsumoto ab. Aus $\mathbf{v} = \mathbf{u}^h$ folgt $\mathbf{uv} = \mathbf{u}^{q^\theta}\mathbf{u}^{q^\varphi}$, dies ist im $\mathbb{F}_q$ durch lineare Transformationen darstellbar. Letztendlich folgen durch die bekannten Umformungen

$$\sum_{1\le i,j\le n} u_i v_j \beta_i \beta_j = \left(\sum_{1\le i,\mu\le n} p_{i\mu}^{(\theta)} u_i \beta_\mu\right)\left(\sum_{1\le j,\nu\le n} p_{j\nu}^{(\varphi)} u_j \beta_\nu\right)$$

die $l = 1, \ldots, n$ Gleichungen

$$\sum_{1\le i,j\le n} m_{ijl} u_i v_j = \sum_{1\le i,j,\mu,\nu\le n} p_{i\mu}^{(\theta)} p_{j\nu}^{(\varphi)} m_{\mu\nu l} u_i u_j$$

und daraus durch Einsetzen der Transformationsgleichungen $\vec{u} = A\vec{x}$, $\vec{v} = B\vec{y}$ und durch Koeffizientenumbenennung die $l = 1, \ldots, n$ zu veröffentlichenden Gleichungen

$$\sum_{1\le i,j\le n} c_{ijl} x_i y_j + \sum_{1\le i\le j\le n} d_{ijl} x_i x_j = 0.$$

Der Sender setzt einen Klartext $\vec{x}$ ein, dadurch wird das System linear, und löst die Gleichungen mit dem Gaußschen Eliminationsverfahren nach $\vec{y}$, dem Chiffrat. Der legitime Empfänger kann durch die geheimen Parameter die Operationen umkehren und $\vec{x}$ einfach berechnen. Ein Angreifer steht zunächst vor einem nichtlinearen Gleichungssystem.

1.3.2 Schwache Exponenten

Bei der Wahl des Exponenten h im n-dimensionalen Erweiterungskörper $\mathbb{K}$ von $\mathbb{F}_q$ muß im Fall $q = 2$ beachtet werden, daß schwache Exponenten existieren. In diesen Fällen ist ein einfach durchführbarer Angriff möglich, der im folgenden skizziert wird.
Der Exponent h ist wieder von der Form $h = 2^\theta + 2^\varphi - 1$, zusätzlich gilt $ggT(h, 2^n - 1) = 1$. Aus der zentralen Gleichung $\mathbf{v} = \mathbf{u}^h$ kann man durch Potenzieren mit γ, wobei $ggT(\gamma, 2^n - 1) = 1$, und Multiplizieren mit Potenzen von $\mathbf{u}$ und $\mathbf{v}$ die Gleichung

$$\mathbf{v}^{2^{i_1}}\mathbf{v}^{2^{i_2}}\ldots\mathbf{v}^{2^{i_k}}\mathbf{u}^{2^\alpha} = \mathbf{v}^{2^{j_1}}\mathbf{v}^{2^{j_2}}\ldots\mathbf{v}^{2^{j_{k'}}}u^{2^\beta}$$

erhalten, wobei kleine Werte für k und k' ausreichen. Im $\mathbb{F}_2$ sind Abbildungen der Form $v \mapsto v^{2^i}$ linear darstellbar. Die obige Gleichung kann deshalb nach dem Einsetzen eines abgefangenen Chiffrats $\vec{y}$ zu einem linearen, leicht nach dem Klartext $\vec{x}$ zu lösenden Gleichungssystem transformiert werden. Für diesen Spezialfall ist das Krypto-System gebrochen.

1.3.3 Angriffsversuch

Dieser Abschnitt schildert einen naiven einfachen Angrifssversuch, der so nicht funktionieren kann. Es kann angenommen werden, dass der Angreifer den Exponenten h kennt, da es hierzu nur wenige Möglichkeiten gibt. Unbekannt sind also nur die Basis $\vec{\beta}$ und die Transformationsmatrizen A und B.
Der Angriff wird durch die Wahl eine beliebigen Basis $\vec{\beta}'$ gestartet. Es wird versucht zu $\vec{\beta}'$ passende A' und B' zu bestimmen, die dasselbe leisten wie A und B bezüglich Basis $\vec{\beta}$.
Die folgende Gleichung ist somit der Ausgangspunkt:

$$\sum_{1\leq i,j\leq n} m'_{ijl}u_iv_j = \sum_{1\leq i,j,\mu,\nu\leq n} {p'_{i\mu}}^{(\theta)}{p'_{j\nu}}^{(\varphi)}m'_{\mu\nu l}u_iu_j,$$

wobei sich durch die andere Basiswahl auch andere Koeffizientenwerte ergeben. Als nächstes müssen die Transformationen berücksichtigt werden. Der Angreifer erzeugt eine große Anzahl $2n$-Tupel $(x_1,\ldots,x_n,y_1,\ldots,y_n)$ Klartext-/Schlüsseltext-Paare und setzt sie in $\vec{u} = A'\vec{x}$ und $\vec{v} = B'\vec{y}$ ein. Er erhält n quadratische Gleichungen mit den $2n^2$ Unbekannten a'_{ij} und b'_{ij} der noch nicht bekannten Matrizen A' und B'.

$$\sum_{i,j=1}^{n} m'_{ijl}(\sum_{\mu,\nu=1}^{n} a'_{i\mu}x_\mu b'_{j\nu}y_\nu) = \sum_{i,j,k,m=1}^{n} {p'_{ik}}^{(\theta)}{p'_{jm}}^{(\varphi)}m'_{kml}(\sum_{\mu,\omega=1}^{n} a'_{i\mu}x_\mu a'_{j\omega}x_\omega)$$

Die Produkte $a'_{ij}b'_{kl}$ und $a'_{ij}a'_{kl}$ werden durch $O(n^4)$ neue Variablen ersetzt. Gelingt es, alle $O(n^4)$ Variablen zu bestimmen, so ist das System gebrochen. Doch dazu braucht man $O(n^4)$ unabhängige Gleichungen. Was passiert, wenn man nun nur $O(n^3)$ Gleichungen bekommt? Hier kann man nicht damit argumentieren, das der Lösungsraum mit weniger Gleichungen schon entscheidend verkleinert werden kann. Das kann man sich an folgender kleiner Aufgabe klarmachen: Löse $w_1 = a_1a_2 = c_1, w_2 = a_1b_1 = c_2, w_3 = a_2b_1 = c_3$ nach a_1, a_2, b_1, wenn nicht alle Werte c_i bekannt sind.
Wie [1] zeigt, gewinnt ein Angreifer nur $3/2n^3 + 1/2n^2$ Gleichungen, das ist nicht genug, und damit scheitert der Angriff.

1.3.4 Kryptanalyse

Schon kurz nach der Veröffentlichung des Little Dragon fanden Coppersmith und Patarin eine universelle Angriffsmethode [3]. Das Prinzip dieses Angriffs wird hier vorgestellt, der ausführliche Beweis findet sich wieder in [1]. Es wird eine bilineare Abbildung auf Y (dem Vektorraum der Chiffrate $\vec{y} = (y_1,\ldots,y_n)$) konstruiert:

$$(\vec{y},\vec{y'}) \mapsto \vec{y''} := \vec{y} \diamond \vec{y'}$$

so dass mit

$$\vec{v}^j := B\vec{y}^j$$

gilt:

$$\mathbf{v}'' = \mu\mathbf{v}\mathbf{v}'$$

für ein festes $\mu \in \mathbb{K}$, $(\mu \neq 0)$. Eine solche Abbildung existiert. Eine weitere Definition ist nötig: $\vec{y}^{(j)} = \vec{y}\diamond\vec{y}^{(j-1)}$. Eine wiederholte Anwendung von $\diamond$ führt zu: $\mathbf{v}^{(j)} = \mu\mathbf{v}\mathbf{v}^{j-1} = \mu^2\mathbf{v}\mathbf{v}\mathbf{v}^{j-2} = \ldots = \mu^{j-1}\mathbf{v}^j$. Speziell gilt diese Gleichung für $j = h'$ (h' ist das multiplikative Inverse zu h mod $q^n - 1$):

$$\mathbf{v}^{(h')} = \mu^{h'-1}\mathbf{v}^{h'}$$

und damit

$$\mathbf{u} = \mathbf{v}^{h'} = \mu^{-(h'-1)}\mathbf{v}^{(h')}.$$

Elemente aus $\mathbb{K}$, z.B. $\mu^{-(h'-1)}$ kann man wieder zu Vektoren aus $\mathbb{F}_q^n$ zurücktransformieren. Die Matrix M sei die Multiplikationsmatrix von diesem Vektor mit der Basis. Dann gilt:

$$\vec{x} = A^{-1}\vec{u} = A^{-1}M\vec{v}^{(h')} = A^{-1}MB\vec{y}^{(h')}$$

wobei $A^{-1}MB$ eine feste Matrix ist und somit $A^{-1}MB = C$ gesetzt werden kann. Es gilt

$$\vec{x} = C\vec{y}^{(h')}.$$

C ist unbekannt, da auch die Basis $\beta_1, \ldots, \beta_n$ unbekannt ist. Jedoch gilt wieder die übliche Annahme, dass einem Angreifer der Exponent h (und damit auch h') bekannt sind, beispielsweise durch Ausprobieren der wenigen Belegungsmöglichkeiten. Betrachte die letzte Gleichung etwas genauer:

$$x = Cy^{(h')}.$$

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} c_{11} & \ldots & c_{1n} \\ \vdots & \ddots & \vdots \\ c_{n1} & \ldots & c_{nn} \end{pmatrix} \begin{pmatrix} y_1^{(h)} \\ \vdots \\ y_n^{(h)} \end{pmatrix}$$

Der Angriff läuft wieder darauf hinaus, mit Schlüsseltext-Paaren zu arbeiten. Jedes $2n$-Tupel erzeugt n Gleichungen, um die n^2 Unbekannten c_{ij} zu bestimmen. Mit $O(n)$ dieser Tupel wird das gelingen. Damit ist eine direkte Abbildung gefunden, die einen verschlüsselten Text auf den zugrundeliegenden Klartext abbildet. Das Little-Dragon-System ist gebrochen.

Literaturverzeichnis

[1] N. Koblitz: *Algebraic Aspects of Cryptography*, Springer Verlag 1998

[2] H. Imai, T. Matsumoto: *Public Quadratic Polynomial-Tuples for Efficient Signature-Verification and Message-Encryption, Advances in Cryptology – Eurocrypt 1988*, Springer Verlag, 419-453

[3] J. Patarin: *Asymmetric Cryptography with a Hidden Monomial, Advances in Cryptology – Crypt 1996*, Springer Verlag, 45-60

[4] J. Patarin: *Cryptanalysis of the Matsumoto and Imai Public Key Scheme of Eurocrypt 1988, Advances in Cryptology – Crypto 1995*, Springer Verlag, 248-261

[5] E. R. Berlekamp: *Algebraic Coding Theory*, McGraw-Hill, 1968

[6] L. Goubin, J. Patarin: *Trapdoor One-Way Permutations and Multivariate Polynomials – Lecture Notes in Computer Science, Vol. 1334, November 1997*, Springer Verlag, 356-368