Universität Paderborn
Fakultät für Elektrotechnik, Informatik und Mathematik

Behandlung von Korrekturtermen in der Methode von Coppersmith

Abschlussarbeit von Stefan Birkner

Hiermit erkläre ich, dass ich diese Arbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe.

Paderborn, den 1. März 2007

Inhaltsverzeichnis

1 Einleitung

Durch die zunehmende Nutzung des Internets besteht ein Interesse daran, Daten sicher zu übertragen. Die Kryptografie stellt die dafür notwendigen Verfahren zur Verfügung. Unter diesen ist das, nach seinen Erfindern Rivest, Shamir und Adleman benannte, RSA-Verfahren besonders wichtig. Um Nachrichten zu verschlüsseln, verwendet man einen öffentlich zugänglichen Schlüssel, der aus zwei Zahlen besteht: einem Verschlüsselungsexponenten und einem RSA-Modul, der das Produkt zweier Primzahlen ist. Der Empfänger kennt einen dazu passenden geheimen Entschlüsselungsexponenten, mit dem er aus dem Geheimtext wieder die Originalnachricht berechnen kann.

Seit der Veröffentlichung des RSA-Verfahrens versuchen Kryptologen herauszufinden, ob es auch ohne Kenntnis des Entschlüsselungsexponenten möglich ist, Geheimtexte zu entschlüsseln. Dies gelingt mittlerweile bei sogenannten Gitterangriffen, wenn ein Teil des Entschlüsselungsexponenten oder eines der beiden Faktoren des RSA-Moduls bekannt ist. Dazu konstruiert man aus den bekannten Informationen spezielle Polynome und berechnet deren ganzzahlige Nullstellen. Mit den Nullstellen ist es letztendlich möglich die Geheimtexte zu entschlüsseln.

Zur Berechnung der Nullstellen wird ein Verfahren verwendet, das Don Coppersmith Mitte der neunziger Jahre veröffentlichte. Damit die Gitterangriffe erfolgreich sind, muss ein ebenfalls von ihm stammendes Korollar gelten, für dessen Beweis er das Verfahren geringfügig modifizierte. Da diese Modifikation nur in zwei Sätzen beschrieben wurde, besteht Unklarheit über deren Beschaffenheit und die Gültigkeit des Korollars.

Die Aufgabenstellung dieser Abschlussarbeit besteht darin, das Korollar zu beweisen indem aus der Idee des modifizierten Verfahrens ein konkretes Verfahren entwickelt wird. Wir beschreiben dazu zuerst welche Nullstellen das Basisverfahren berechnet und stellen das Korollar vor. Anschließend zeigen wir, dass dieses durch eine naheliegende Modifikation des Basisverfahrens nicht bewiesen werden kann. Der Beweis scheitert daran, dass eine bestimmte Schranke zu eng gefasst ist. Indem wir das Verhalten der Schranke analysieren, erhalten wir ein modifiziertes Verfahren, mit dem wir die Gültigkeit des Korollars beweisen.

2 Verwendete Begriffe und Symbole

In dieser Arbeit verwenden wir einige spezielle Begriffe und Symbole. Das Ziel ist stets ganzzahlige Nullstellen (x_0, y_0) eines bivariaten Polynoms $p(x, y)$ zu berechnen. Dieses hat in beiden Variablen jeweils höchstens den Grad δ. Seine Koeffizienten werden mit p_{ij} bezeichnet.

$$p(x, y) = \sum_{i=0}^{\delta} \sum_{j=0}^{\delta} p_{ij} x^i y^j$$

Es werden nur Nullstellen berechnet, die innerhalb eines rechteckigen Bereichs $D_{X,Y}$ liegen, dessen Grenzen durch X und Y festgelegt sind.

$$D_{X,Y} = \{(x, y) \,|\, |x| \leq X, |y| \leq Y\}$$

In Abhängigkeit von den Schranken X und Y lässt sich die für das Verfahren wichtige Größe $W(X,Y)$ berechnen.

$$W(X,Y) = \max\{\, |p_{ij}|X^iY^j \mid 0 \le i \le \delta, 0 \le j \le \delta \,\}$$

Sie entspricht dem betragsmäßig größten Koeffizienten des Polynoms $\tilde{p}(x,y) = p(xX, yY)$. Gehen die Schranken X und Y eindeutig aus dem Zusammenhang hervor, so schreiben wir anstatt $W(X,Y)$ auch W.

Das Polynom $p(x,y)$ wird innerhalb dieser Arbeit mehrfach in der x-Richtung um einen Verschiebungsvektor $a \in [-X;X]$ verschoben. Das verschobene Polynom bezeichnen wir mit $p_a(x,y)$ und seine Koeffizienten mit $p_{ij,a}$.

$$p_a(x,y) = p(x+a,y) = \sum_{i=0}^{\delta}\sum_{j=0}^{\delta} p_{ij,a}x^iy^j$$

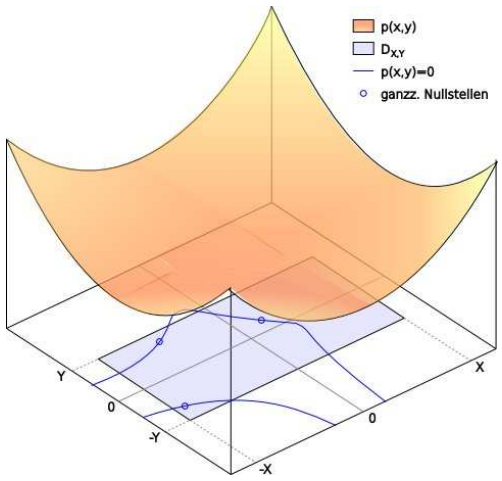
Für dieses Polynom lässt sich wieder die Größe $W(X,Y)$ berechnen. Zur besseren Unterscheidung bezeichnen wir sie mit $W_a(X,Y)$ oder W_a, wenn die Schranken X und Y aus dem Zusammenhang ersichtlich sind.

$$W_a(X,Y) = \max\{\, |p_{ij,a}|X^iY^j \mid 0 \le i \le \delta, 0 \le j \le \delta \,\}$$

3 Das Basisverfahren

Ausgangspunkt unserer Überlegung ist das unmodifizierte Verfahren von Coppersmith, das wir im Weiteren Basisverfahren nennen. Es wird in [1] beschrieben, dort findet sich auch ein Beweis für seine Korrektheit.

Das Basisverfahren berechnet alle ganzzahligen Nullstellen (x_0, y_0) eines irreduziblen, bivariaten Polynoms $p(x,y)$, die innerhalb des durch X und Y festgelegten Bereichs $D_{X,Y}$ liegen. Das folgende Bild zeigt ein Beispiel, bei dem sich innerhalb von $D_{X,Y}$ drei ganzzahlige Nullstellen befinden.



Die Schranken X und Y können frei gewählt werden, solange ihr Produkt der Bedingung

$$XY < W(X,Y)^{\frac{2}{3\delta}-\varepsilon} \cdot 2^{-\frac{14}{3}\delta} \tag{1}$$

genügt. Der Parameter ε kann ebenfalls frei gewählt werden und beeinflusst die Laufzeit des Verfahrens. Mit seiner Hilfe kann man den Bereich $D_{X,Y}$ vergrößern, wenn man dafür eine längere Laufzeit in Kauf nimmt.

Die Laufzeit des Verfahrens ist polynomiell in $(\log W, \delta, 1/\varepsilon)$, wie ebenfalls in [1] gezeigt wird. Es gibt demnach nichtnegative ganze Zahlen e_1, e_2 und e_3, sodass das Verfahren in Zeit

$$\mathcal{O}((\log W)^{e_1} \cdot \delta^{e_2} \cdot (1/\varepsilon)^{e_3}) \tag{2}$$

Nullstellen berechnet.

4 Das Korollar von Coppersmith

Das Korollar, das wir in dieser Arbeit beweisen, erscheint in [1, S. 251] als Korollar 2 direkt im Anschluss an das Basisverfahren. Es lautet

Korollar 1 (Coppersmith)**.** *Sei $p(x,y)$ ein irreduzibles Polynom in zwei Variablen über $\mathbb{Z}$ vom Höchstgrad δ in jeder einzelnen Variable. Seien X, Y Schranken für die erwünschten Nullstellen x_0, y_0. Definiere $\tilde{p}(x,y) = p(xX, yY)$ und sei W der Betrag des größten Koeffizienten von $\tilde{p}$. Wenn*

$$XY < W^{\frac{2}{3\delta}}$$

gilt, dann können wir in Zeit polynomiell in $(\log W, 2^\delta)$ alle ganzzahligen Paare (x_0, y_0) mit $p(x_0, y_0) = 0$, $|x_0| < X$ und $|y_0| < Y$ finden.

Um dieses Korollar zu beweisen, schlägt Coppersmith vor den Parameter $\varepsilon = 1/\log W$ zu wählen und „eine vollständige Suche auf den obersten $\mathcal{O}(\delta)$ unbekannten Bits von x“ [1] durchzuführen.

Es erscheint naheliegend, dazu den Bereich $D_{X,Y}$ in mehrere kleinere Bereiche $D^{(a)}_{X',Y}$ mit

$$X' = \lfloor 2^{-\frac{14}{3}\delta} X \rfloor$$

zu unterteilen und dort jeweils ganzzahlige Nullstellen zu suchen. Ist a der Mittelpunkt eines solchen Bereichs

$$D^{(a)}_{X',Y} = \{(x,y) \,|\, |x-a| \leq X', |y| \leq Y\}$$

dann verschiebt man das Polynom $p(x,y)$ in x-Richtung jeweils um $-a$ auf das Polynom $p_{-a}(x,y)$. Auf dieses Polynom wendet man das Basisverfahren mit dem angegebenen Parameter ε an, um die ganzzahligen Nullstellen innerhalb des Bereichs $D_{X',Y}$ zu finden. Ist $(x_0^{(a)}, y_0)$ eine so gefunden Nullstelle, so ist $(x_0^{(a)} + a, y_0)$ eine ganzzahlige Nullstelle des Polynoms $p(x,y)$.

Damit das Basisverfahren für die Polynome $p_a(x, y)$ alle Nullstellen berechnet, muss gemäß (1)

$$X'Y < W_a(X', Y)^{\frac{2}{3\delta}-(1/\log W)} \cdot 2^{-\frac{14}{3}\delta}$$

gelten. Solange $W_a(X, Y)$ groß genug ist, trifft dies auch zu. Es gibt jedoch Polynome und Schranken X und Y bei denen $W_a(X, Y)$ so klein wird, dass die Ungleichung nicht mehr erfüllt ist.

Wir betrachten im Folgenden $W_a(X, Y)$ genauer und werden feststellen, dass es im Bezug auf $W(X, Y)$ nicht beliebig klein wird. Darauf aufbauend wählen wir ein gegenüber X' kleineres $\tilde{X}$ und setzen jeweils $\varepsilon = 1/\log W_a$. Führt man jetzt die beschriebene Unterteilung des Bereichs $D_{X,Y}$ durch, treten keine Probleme auf. Nun ist das $W_a(X, Y)$ der verschobenen Polynome groß genug, um die Ungleichung zu erfüllen, sodass das Basisverfahren durchgeführt werden kann.

5 Abschätzungen für W_a

Da $W_a(X, Y)$ neben a auch von X und Y abhängt und X und Y beliebig klein sein können, kann $W_a(X, Y)$ nicht absolut abgeschätzt werden. Stattdessen werden wir für beliebige X und Y zeigen, um welchen Faktor $W_a(X, Y)$ gegenüber $W(X, Y)$ abfallen kann. Dabei beschränken wir a auf das Intervall $[-X; X]$, da nur diese Werte für das modifizierte Verfahren von Interesse sind.

Wir werden zuerst den Fall $\delta = 1$ ausführlich betrachten, da er einerseits anschaulich zeigt, wie sich $W_a(X, Y)$ bei unterschiedlichen a verändert und andererseits den in der Praxis bei Gitterangriffen am häufigsten auftretenden Fall darstellt. Der Fall $\delta = 2$ führt zu einer Abschätzung, der man schon ansieht wie sie sich auf beliebige δ verallgemeinern lässt. Diese Verallgemeinerung führen wir abschließend durch und erhalten einen Satz mit einer entsprechenden Abschätzung.

5.1 W_a bei Polynomen vom Grad 1

In diesem Abschnitt betrachten wir bivariate Polynome vom Grad 1 in beiden Variablen. Die Polynome $p(x, y)$ und die zugehörigen verschobenen Polynome $p_a(x, y)$ sind durch

$$\begin{aligned} p(x, y) &= p_{11}xy + p_{10}x + p_{01}y + p_{00} \\ p_a(x, y) &= p_{11}xy + p_{10}x + (ap_{11} + p_{01})y + (ap_{10} + p_{00}) \end{aligned}$$

gegeben. Wir zeigen, dass sich $W_a(X, Y)$ innerhalb des interessanten Bereichs gegenüber $W(X, Y)$ höchstens halbiert:

$$W_a(X, Y) \geq \frac{1}{2}W(X, Y) \qquad \text{für } a \in [-X; X]$$

Im Speziellen zeigen wir, dass immer mindestens eines der Monome $p_{11}xy$, $p_{10}x$, $(ap_{11} + p_{01})y$ und $(ap_{10} + p_{00})$ mindestens halb so groß wie $W(X, Y)$ ist.

Dazu führen wir eine Fallunterscheidung an Hand der für $W(X,Y)$ ausschlaggebenden Monome durch. Die folgenden drei Fälle treten auf:

- $W(X,Y) = |p_{11}XY|$ oder $W(X,Y) = |p_{10}X|$
- $W(X,Y) = |p_{01}Y|$
- $W(X,Y) = |p_{00}|$

5.1.1 Fall 1: $W(X,Y) = |p_{11}XY|$ oder $W(X,Y) = |p_{10}X|$

Da die Monome $p_{11}xy$ und $p_{10}x$ in beiden Polynomen gleich sind, gilt ohne Einschränkung die Ungleichung

$$W_a(X,Y) \geq W(X,Y) \geq \frac{1}{2}W(X,Y)$$

5.1.2 Fall 2: $W(X,Y) = |p_{01}Y|$

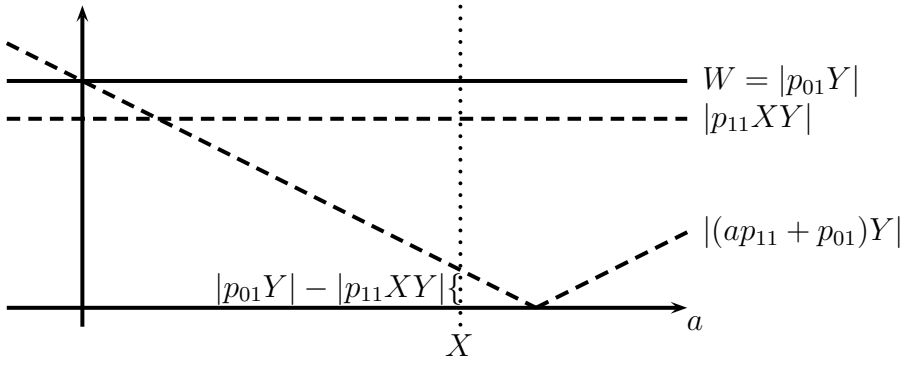
Hier zeigen wir, dass mindestens eines der beiden Monome $p_{11}xy$ und $(ap_{11} + p_{01})y$ die Bedingung erfüllt. Es muss also für $a \in [-X; X]$ mindestens eine der beiden folgenden Ungleichungen gelten:

$$|p_{11}XY| \geq \frac{1}{2}|p_{01}Y|$$
$$|(ap_{11} + p_{01})Y| \geq \frac{1}{2}|p_{01}Y|$$

Da sich der Wert von W aus dem Monom $p_{01}y$ berechnet, muss $|p_{11}XY| \leq |p_{01}Y|$ bzw. $|p_{11}X| \leq |p_{01}|$ gelten. Wir unterscheiden hier noch einmal zwei Fälle. Im ersten Fall besitzen die Koeffizienten p_{11} und p_{01} verschiedene Vorzeichen. Für negative a ist

$$|(ap_{11} + p_{01})Y| = |ap_{11}Y| + |p_{01}Y| \geq |p_{01}Y| = W(X,Y)$$

Für alle $a \in [0; X]$ verhält sich $|(ap_{11} + p_{01})Y|$ wie im folgenden Bild gezeigt. Der Graph von $|(ap_{11} + p_{01})Y|$ kann an Hand der Werte für $a = 0$ und $a = X$ gezeichnet werden.



Es gilt also für alle $a \in [0; X]$

$$\begin{aligned} |(ap_{11} + p_{01})Y| &= |p_{01}Y| - |ap_{11}Y| \\ |(ap_{11} + p_{01})Y| &\geq |p_{01}Y| - |p_{11}XY| \\ |(ap_{11} + p_{01})Y| + |p_{11}XY| &\geq |p_{01}Y| \end{aligned}$$

$$|(ap_{11} + p_{01})Y| \geq \frac{1}{2}|p_{01}Y| \qquad \vee \qquad |p_{11}XY| \geq \frac{1}{2}|p_{01}Y|$$

Es bleibt der Fall, dass die Koeffizienten p_{11} und p_{01} gleiche Vorzeichen haben. Die Argumentation ist die Gleiche, außer dass der interessante Bereich das Intervall $[-X; 0]$ ist.

5.1.3 Fall 3: $W(X, Y) = |p_{00}|$

Hier zeigen wir, dass mindestens eines der beiden Monome $p_{10}x$ und $ap_{10} + p_{00}$ die Bedingung erfüllt. Es muss also für $a \in [-X; X]$ mindestens eine der beiden folgenden Ungleichungen gelten:

$$|p_{10}X| \geq \frac{1}{2}|p_{00}|$$

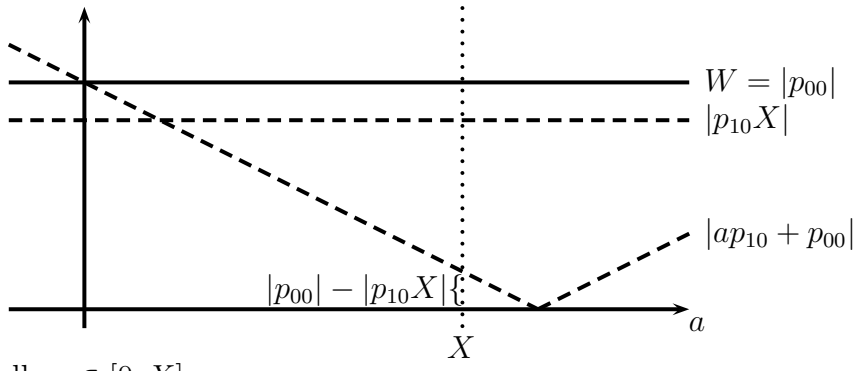
$$|ap_{10} + p_{00}| \geq \frac{1}{2}|p_{00}|$$

Die Argumentation unterscheidet sich kaum vom Fall 2.

Da sich der Wert von W aus dem Monom p_{00} berechnet, muss $|p_{10}X| \leq |p_{00}|$ gelten. Wir unterscheiden wieder zwei Fälle. Im ersten Fall besitzen die Koeffizienten p_{10} und p_{00} verschiedene Vorzeichen. Für negative a ist

$$|ap_{10} + p_{00}| = |ap_{10}| + |p_{00}| \geq |p_{00}| = W(X, Y)$$

Für alle $a \in [0; X]$ verhält sich $|ap_{10} + p_{00}|$ wie im folgenden Bild gezeigt. Der Graph von $|ap_{10} + p_{00}|$ kann an Hand der Werte für $a = 0$ und $a = X$ gezeichnet werden.



Es gilt also für alle $a \in [0; X]$

$$\begin{aligned} |ap_{10} + p_{00}| &= |p_{00}| - |ap_{10}| \\ |ap_{10} + p_{00}| &\geq |p_{00}| - |p_{10}X| \\ |ap_{10} + p_{00}| + |p_{10}X| &\geq |p_{00}| \end{aligned}$$

$$|ap_{10} + p_{00}| \geq \frac{1}{2}|p_{00}| \qquad \vee \qquad |p_{10}X| \geq \frac{1}{2}|p_{00}|$$

Es bleibt noch der Fall, dass die Koeffizienten p_{10} und p_{00} gleiche Vorzeichen haben. Die Argumentation ist die Gleiche, außer dass der interessante Bereich das Intervall $[-X; 0]$ ist.

5.2 W_a bei Polynomen vom Grad 2

Wir betrachten nun bivariate Polynome vom Grad 2 in beiden Variablen. Die Polynome $p(x, y)$ und die zugehörigen verschobenen Polynome $p_a(x, y)$ sind durch

$$\begin{aligned}
p(x,y) &= p_{22}x^2y^2 + p_{21}x^2y + p_{20}x^2 + p_{12}xy^2 + p_{11}xy + p_{10}x + p_{02}y^2 + p_{01}y + p_{00} \\
p_a(x,y) &= p_{22}x^2y^2 + p_{21}x^2y + p_{20}x^2 \\
&\quad + (2ap_{22} + p_{12})xy^2 \\
&\quad + (2ap_{21} + p_{11})xy \\
&\quad + (2ap_{20} + p_{10})x \\
&\quad + (a^2p_{22} + ap_{12} + p_{02})y^2 \\
&\quad + (a^2p_{21} + ap_{11} + p_{01})y \\
&\quad + (a^2p_{20} + ap_{10} + p_{00})
\end{aligned}$$

gegeben. Wir zeigen, dass $W_a(X, Y)$ für $a \in [-X; X]$ gegenüber $W(X, Y)$ höchstens auf ein Drittel sinkt:

$$W_a(X,Y) \geq \frac{1}{3}W(X,Y) \qquad \text{für } a \in [-X; X]$$

Da sich das verschobene Polynom in der Form

$$p_a(x,y) = \sum_{j=0}^{2} p_{2j}x^2y^j + (2ap_{2j} + p_{1j})xy^j + (a^2p_{2j} + ap_{1j} + p_{0j})y^j$$

darstellen lässt, genügt es die drei Fälle $W(X, Y) = |p_{2j}|X^2Y^j$, $W(X, Y) = |p_{1j}|XY^j$ und $W(X, Y) = |p_{0j}|Y^j$ zu betrachten.

Gilt $W(X, Y) = |p_{2j}|X^2Y^j$, dann ist

$$\begin{aligned}
W_a(X,Y) &\geq |p_{2j}|X^2Y^j \\
&= W(X,Y) \\
&> \frac{1}{3}W(X,Y)
\end{aligned}$$

da das $W(X, Y)$ bestimmende Monom $p_{2j}x^2y^j$ auch im Polynom $p_a(x, y)$ auftritt.

Sei nun $W(X, Y) = |p_{1j}|XY^j$. Zusätzlich gelte $|p_{2j,a}|X^2Y^j < \frac{1}{3}W(X, Y)$, denn sonst ist die zu beweisende Ungleichung schon erfüllt. Auf Grund von $|p_{2j,a}|X^2Y^j = |p_{2j}|X^2Y^j$ ist auch

$$|p_{2j}|X^2Y^j < \frac{1}{3}W(X,Y)$$

Da $|a| \leq X$ können wir die Ungleichung

$$|2ap_{2j}|XY^j \leq 2|p_{2j}|X^2Y^j < \frac{2}{3}W(X,Y)$$

verwenden, um $W_a(X,Y)$ abzuschätzen.

$$\begin{aligned} W_a(X,Y) &\geq |p_{1j,a}|XY^j \\ &= |2ap_{2j} + p_{1j}|XY^j \\ &\geq |\,|p_{1j}|XY^j - |2ap_{2j}|XY^j\,| \\ &\geq |W(X,Y) - \frac{2}{3}W(X,Y)| \\ &= \frac{1}{3}W(X,Y) \end{aligned}$$

Sei nun $W(X,Y) = |p_{0j}|Y^j$. Zusätzlich gelte $|p_{2j,a}|X^2Y^j < \frac{1}{3}W(X,Y)$ oder $|p_{1j,a}|XY^j < \frac{1}{3}W(X,Y)$, denn sonst ist die zu beweisende Ungleichung schon erfüllt. Daraus folgt

$$\begin{aligned} |p_{2j,a}|X^2Y^j &= |p_{2j}|X^2Y^j < \frac{1}{3}W(X,Y) \\ |p_{1j,a}|XY^j &= |2ap_{2j} + p_{1j}|XY^j < \frac{1}{3}W(X,Y) \end{aligned}$$

Damit zeigen wir eine Abschätzung für den Term $(a^2p_{2j} + ap_{1j})Y^j$

$$\begin{aligned} |a^2p_{2j} + ap_{1j}|Y^j &= |2a^2p_{2j} - a^2p_{2j} + ap_{1j}|Y^j \\ &\leq |a^2p_{2j}|Y^j + |2a^2p_{2j} + ap_{1j}|Y^j \\ &\leq |p_{2j}|X^2Y^j + |2ap_{2j} + p_{1j}|XY^j \\ &\leq \frac{1}{3}W(X,Y) + \frac{1}{3}W(X,Y) \\ &= \frac{2}{3}W(X,Y) \end{aligned}$$

Mit dieser Abschätzung folgt für $W_a(X,Y)$

$$\begin{aligned} W_a(X,Y) &\geq |p_{0j,a}|Y^j \\ &= |a^2p_{2j} + ap_{1j} + p_{0j}|Y^j \\ &\geq |\,|p_{0j}|Y^j - |a^2p_{2j} + ap_{1j}|Y^j\,| \\ &\geq |W(X,Y) - \frac{2}{3}W(X,Y)| \\ &= \frac{1}{3}W(X,Y) \end{aligned}$$

5.3 W_a bei Polynomen beliebigen Grads

Um für ein Polynom beliebigen Grades eine untere Grenze für $W_a(X, Y)$ in Abhängigkeit von $W(X, Y)$ angeben zu können, betrachten wir, wie sich die einzelnen Monome des verschobenen Polynoms gegenseitig beeinflussen. Als Hilfsmittel verwenden wir dazu eine Darstellung der Koeffizienten des verschobenen Polynoms als Linearkombination der „größeren“ Koeffizienten. Diese werden wir zunächst entwickeln und anschließend eine untere Schranke für $W_a(X, Y)$ bestimmen.

5.3.1 Die Koeffizienten des verschobenen Polynoms

Die Koeffizienten des verschobenen Polynoms lassen sich als Linearkombination der Koeffizienten des ursprünglichen Polynoms darstellen.

Lemma 1. *Es sei $p(x, y)$ ein bivariates Polynom über den ganzen Zahlen vom Höchstgrad δ in beiden Variablen und a eine ganze Zahl. Dann gilt für die Koeffizienten $p_{ij,a}$ des verschobenen Polynoms $p_a(x, y)$*

$$p_{ij,a} = \sum_{k=i}^{\delta} \binom{k}{i} a^{k-i} p_{kj}$$

Beweis. Wir setzen $x + a$ in das ursprüngliche Polynom ein.

$$\begin{aligned}
p_a(x, y) &= p(x + a, y) \\
&= \sum_{i=0}^{\delta} \sum_{j=0}^{\delta} p_{ij} (x + a)^i y^j \\
&= \sum_{i=0}^{\delta} \sum_{j=0}^{\delta} p_{ij} \cdot \left(\sum_{k=0}^{i} \binom{i}{k} a^{i-k} x^k \right) \cdot y^j \\
&= \sum_{i=0}^{\delta} \sum_{j=0}^{\delta} \sum_{k=0}^{i} \binom{i}{k} a^{i-k} p_{ij} x^k y^j \\
&= \sum_{k=0}^{\delta} \sum_{j=0}^{\delta} \sum_{i=k}^{\delta} \binom{i}{k} a^{i-k} p_{ij} x^k y^j \\
&= \sum_{i=0}^{\delta} \sum_{j=0}^{\delta} \underbrace{\sum_{k=i}^{\delta} \binom{k}{i} a^{k-i} p_{kj} x^i y^j}_{= p_{ij,a}}
\end{aligned}$$

□

Daneben lässt sich für die Koeffizienten $p_{ij,a}$ noch eine weitere Darstellung als Linearkombination von p_{ij} und den $p_{kj,a}$ mit $k > i$ finden.

Lemma 2. *Es sei $p(x,y)$ ein bivariates Polynom über den ganzen Zahlen vom Höchstgrad δ in beiden Variablen und a eine ganze Zahl. Dann gilt für die Koeffizienten $p_{ij,a}$ des verschobenen Polynoms $p_a(x,y)$*

$$p_{ij,a} = p_{ij} + \sum_{k=i+1}^{\delta} (-1)^{k-i+1} \binom{k}{i} a^{k-i} p_{kj,a}$$

Beweis. Wir nehmen an, dass es Linearfaktoren d_k mit

$$p_{ij,a} = p_{ij} + \sum_{k=i+1}^{\delta} d_k a^{k-i} p_{kj,a} \tag{3}$$

gibt und berechnen diese.

Indem man in dieser Gleichung die $p_{kj,a}$ jeweils durch die Formel aus Lemma 1 ersetzt, gelangt man zu folgender Darstellung:

$$\begin{aligned} p_{ij,a} &= p_{ij} + \sum_{k=i+1}^{\delta} d_k a^{k-i} \cdot \sum_{l=k}^{\delta} \binom{l}{k} a^{l-k} p_{lj} \\ &= p_{ij} + \sum_{k=i+1}^{\delta} \sum_{l=k}^{\delta} d_k a^{l-i} \binom{l}{k} p_{lj} \\ &= p_{ij} + \sum_{l=i+1}^{\delta} \sum_{k=i+1}^{l} d_k a^{l-i} \binom{l}{k} p_{lj} \end{aligned}$$

Ein Koeffizientenvergleich mit der ebenfalls aus Lemma 1 hervorgehenden Gleichung

$$p_{ij,a} = p_{ij} + \sum_{l=i+1}^{\delta} \binom{l}{i} a^{l-i} p_{lj}$$

zeigt, dass für alle l mit $i+1 \leq l \leq \delta$ die Gleichung

$$\begin{aligned} \binom{l}{i} a^{l-i} &= \sum_{k=i+1}^{l} d_k a^{l-i} \binom{l}{k} \\ \binom{l}{i} &= \sum_{k=i+1}^{l} d_k \binom{l}{k} \end{aligned}$$

gelten muss. Dies führt auf das lineare Gleichungssystem

$$\begin{pmatrix} \binom{\delta}{\delta} & \binom{\delta}{\delta-1} & \binom{\delta}{\delta-2} & \cdots & \binom{\delta}{i+2} & \binom{\delta}{i+1} \\ 0 & \binom{\delta-1}{\delta-1} & \binom{\delta-1}{\delta-2} & \cdots & \binom{\delta-1}{i+2} & \binom{\delta-1}{i+1} \\ 0 & 0 & \binom{\delta-2}{\delta-2} & \cdots & \binom{\delta-2}{i+2} & \binom{\delta-2}{i+1} \\ & \vdots & & \ddots & & \vdots \\ 0 & 0 & 0 & \cdots & \binom{i+2}{i+2} & \binom{i+2}{i+1} \\ 0 & 0 & 0 & \cdots & 0 & \binom{i+1}{i+1} \end{pmatrix} \cdot \begin{pmatrix} d_\delta \\ d_{\delta-1} \\ d_{\delta-2} \\ \vdots \\ d_{i+2} \\ d_{i+1} \end{pmatrix} = \begin{pmatrix} \binom{\delta}{i} \\ \binom{\delta-1}{i} \\ \binom{\delta-2}{i} \\ \vdots \\ \binom{i+2}{i} \\ \binom{i+1}{i} \end{pmatrix}$$

Die Binomialkoeffizienten auf der Hauptdiagonalen der Koeffizientenmatrix sind alle 1 und damit auch die Determinante. Da 1 eine Einheit in $\mathbb{Z}$ ist, ist das Gleichungssystem eindeutig durch ganze Zahlen lösbar. Des Weiteren handelt es sich bei der Koeffizientenmatrix um eine rechte obere Dreiecksmatrix, sodass sich die Lösung des Gleichungssystems nach folgender Formel berechnet:

$$d_k = \binom{k}{i} - \sum_{l=i+1}^{k-1} \binom{k}{l} d_l \qquad k = i+1, i+2, \ldots, \delta$$

Darauf aufbauend lässt sich mittels vollständiger Induktion zeigen, dass

$$d_k = (-1)^{k-i+1} \binom{k}{i} \qquad k = i+1, i+2, \ldots, \delta$$

gilt. Der Induktionsanfang für $k = i+1$ ist offensichtlich, da die Summe in diesem Fall leer ist.

$$\begin{aligned}
d_k &= \binom{k}{i} - \sum_{l=i+1}^{k-1} \binom{k}{l} d_l \\
&= \binom{k}{i} - \sum_{l=i+1}^{k-1} (-1)^{l-i+1} \binom{k}{l} \binom{l}{i} \\
&= \binom{k}{i} - \sum_{l=1}^{k-i-1} (-1)^{l+1} \binom{k}{l+i} \binom{l+i}{i} \\
&= \binom{k}{i} + \sum_{l=1}^{k-i-1} (-1)^{l} \frac{k!}{(k-l-i)! \cdot l! \cdot i!} \\
&= \binom{k}{i} + \sum_{l=1}^{k-i-1} (-1)^{l} \frac{(k-i)!}{(k-l-i)! \cdot l!} \cdot \frac{k!}{(k-i)! \cdot i!} \\
&= \underbrace{(-1)^0 \binom{k-i}{0}}_{=1} \binom{k}{i} + \left(\sum_{l=1}^{k-i-1} (-1)^l \binom{k-i}{l} \right) \cdot \binom{k}{i} \\
&= \left(\sum_{l=0}^{k-i-1} (-1)^l \binom{k-i}{l} \right) \cdot \binom{k}{i} \\
&= \underbrace{\left(\sum_{l=0}^{k-i} (-1)^l \binom{k-i}{l} \right)}_{=0} \cdot \binom{k}{i} - (-1)^{k-i} \binom{k-i}{k-i} \binom{k}{i} \\
&= (-1)^{k-i+1} \binom{k}{i}
\end{aligned}$$

Setzen wir diese Formel für die d_k in Gleichung (3) ein, so erhalten wir Gleichung von Lemma 2.

□

5.4 Eine untere Schranke für $W_a(\tilde{X}, Y)$

Satz 1. *Es sei $p(x, y)$ ein bivariates Polynom über den ganzen Zahlen vom Höchstgrad δ in beiden Variablen, a eine ganze Zahl und X, $\tilde{X}$ und Y positive ganze Zahlen mit $\tilde{X} \leq X$. Des Weiteren sei*

$$\begin{aligned} W(X, Y) &= \max\{|p_{ij}|X^i Y^j | 0 \leq i \leq \delta, 0 \leq j \leq \delta\} \\ &= |p_{sj}|X^s Y^j \end{aligned}$$

für ein beliebiges aber festes s und j.
Dann gilt für

$$W_a(\tilde{X}, Y) = \max\{|p_{ij,a}|\tilde{X}^i Y^j | 0 \leq i \leq \delta, 0 \leq j \leq \delta\}$$

die Ungleichung

$$W_a(\tilde{X}, Y) \geq \left(\frac{\tilde{X}}{X}\right)^{\delta} \left[\binom{\delta+1}{s+1}\right]^{-1} W(X, Y)$$

für alle $|a| \leq X$.

Beweis. Es sei

$$|p_{ij,a}|\tilde{X}^i Y^j < \left(\frac{\tilde{X}}{X}\right)^{\delta} \left[\binom{\delta+1}{s+1}\right]^{-1} W(X, Y) \qquad i = s+1, s+2, \ldots, \delta$$

denn sonst gilt bereits

$$W_a(\tilde{X}, Y) \geq |p_{ij,a}|\tilde{X}^i Y^j \geq \left(\frac{\tilde{X}}{X}\right)^{\delta} \left[\binom{\delta+1}{s+1}\right]^{-1} W(X, Y)$$

für mindestens ein i und der Satz ist erfüllt.

Wir zeigen, dass

$$|p_{sj,a}|\tilde{X}^s Y^j \geq \left(\frac{\tilde{X}}{X}\right)^{\delta} \left[\binom{\delta+1}{s+1}\right]^{-1} W(X, Y)$$

und damit die Ungleichung des Satzes gilt. Um eine untere Schranke für $|p_{sj,a}|\tilde{X}^s Y^j$ zu finden verwenden wir die Formel aus Lemma 2:

$$p_{sj,a}\tilde{X}^s Y^j = p_{sj}\tilde{X}^s Y^j + \sum_{k=s+1}^{\delta} (-1)^{k-s+1} \binom{k}{s} a^{k-s} p_{kj,a}\tilde{X}^s Y^j$$

Die darin auftretende Summe ist nach oben begrenzt durch

$$
\begin{aligned}
&\left|\sum_{k=s+1}^{\delta}(-1)^{k-s+1}\binom{k}{s}a^{k-s}p_{kj,a}\tilde{X}^sY^j\right| \\
&\leq \sum_{k=s+1}^{\delta}\binom{k}{s}|a|^{k-s}|p_{kj,a}|\tilde{X}^sY^j \\
&\leq \sum_{k=s+1}^{\delta}\binom{k}{s}X^{k-s}|p_{kj,a}|\tilde{X}^sY^j \\
&= \sum_{k=s+1}^{\delta}\binom{k}{s}X^{k-s}\tilde{X}^{s-k}|p_{kj,a}|\tilde{X}^kY^j \\
&= \sum_{k=s+1}^{\delta}\binom{k}{s}\left(\frac{X}{\tilde{X}}\right)^{k-s}|p_{kj,a}|\tilde{X}^kY^j \\
&\leq \sum_{k=s+1}^{\delta}\binom{k}{s}\left(\frac{X}{\tilde{X}}\right)^{\delta-s}|p_{kj,a}|\tilde{X}^kY^j \\
&\leq \sum_{k=s+1}^{\delta}\binom{k}{s}\left(\frac{X}{\tilde{X}}\right)^{\delta-s}\left(\frac{\tilde{X}}{X}\right)^{\delta}\left[\binom{\delta+1}{s+1}\right]^{-1}W(X,Y) \\
&= \left[\sum_{k=1}^{\delta-s}\binom{s+k}{s}\right]\cdot\left(\frac{X}{\tilde{X}}\right)^{-s}\cdot\left[\binom{\delta+1}{s+1}\right]^{-1}W(X,Y) \\
&= \left[\binom{\delta+1}{s+1}-1\right]\cdot\left(\frac{\tilde{X}}{X}\right)^{s}\cdot\left[\binom{\delta+1}{s+1}\right]^{-1}W(X,Y) \\
&= \left(\frac{\tilde{X}}{X}\right)^{s}\cdot\left(1-\left[\binom{\delta+1}{s+1}\right]^{-1}\right)W(X,Y) \\
&= \left(\frac{\tilde{X}}{X}\right)^{s}W(X,Y)-\left(\frac{\tilde{X}}{X}\right)^{s}\left[\binom{\delta+1}{s+1}\right]^{-1}W(X,Y)
\end{aligned}
$$

Mit dieser Abschätzung lässt sich zeigen, dass die Aussage des Satzes gilt.

$$
\begin{aligned}
W_a(X,Y) &\geq |p_{sj,a}|\tilde{X}^s Y^j \\
&\geq \left| |p_{sj}|\tilde{X}^s Y^j - \left| \sum_{k=s+1}^{\delta} (-1)^{k-s+1} \binom{k}{s} a^{k-s} p_{kj,a} \tilde{X}^s Y^j \right| \right| \\
&= \left| \left(\frac{\tilde{X}}{X}\right)^s \cdot |p_{sj}| X^s Y^j - \left| \sum_{k=s+1}^{\delta} (-1)^{k-s+1} \binom{k}{s} a^{k-s} p_{kj,a} \tilde{X}^s Y^j \right| \right| \\
&\geq \left| \left(\frac{\tilde{X}}{X}\right)^s \cdot W(X,Y) - \left(\frac{\tilde{X}}{X}\right)^s \cdot W(X,Y) + \left(\frac{\tilde{X}}{X}\right)^s \cdot \left[\binom{\delta+1}{s+1}\right]^{-1} W(X,Y) \right| \\
&= \left(\frac{\tilde{X}}{X}\right)^s \cdot \left[\binom{\delta+1}{s+1}\right]^{-1} W(X,Y) \\
&\geq \left(\frac{\tilde{X}}{X}\right)^\delta \cdot \left[\binom{\delta+1}{s+1}\right]^{-1} W(X,Y)
\end{aligned}
$$

□

Da stets $s \geq 0$ gilt, lässt sich aus dem vorhergehenden Satz ein von s unabhängiges Korollar ableiten.

Korollar 2. *Es sei $p(x,y)$ ein bivariates Polynom über den ganzen Zahlen vom Höchstgrad δ in beiden Variablen, a eine ganze Zahl und X, $\tilde{X}$ und Y positive ganze Zahlen mit $\tilde{X} \leq X$. Dann gilt*

$$W_a(\tilde{X}, Y) \geq 2^{-(\delta+1)} \left(\frac{\tilde{X}}{X}\right)^\delta W(X,Y)$$

für alle $|a| \leq X$.

Dabei wird der Binomialkoeffizient $\delta + 1$ über $s + 1$ durch $2^{\delta+1}$ abgeschätzt.

6 Beweis des Korollars von Coppersmith

Aufbauend auf der Abschätzung aus Korollar 2 können wir nun das schon einmal oben aufgeführte Korollar von Coppersmith beweisen.

Korollar 3 (Coppersmith)**.** *Sei $p(x,y)$ ein irreduzibles Polynom in zwei Variablen über $\mathbb{Z}$ vom Höchstgrad δ in jeder einzelnen Variable. Seien X, Y Schranken für die erwünschten Nullstellen x_0, y_0. Definiere $\tilde{p}(x,y) = p(xX, yY)$ und sei W der Betrag des größten Koeffizienten von $\tilde{p}$. Wenn*

$$XY < W^{\frac{2}{3\delta}}$$

gilt, dann können wir in Zeit polynomiell in $(\log W, 2^\delta)$ alle ganzzahligen Paare (x_0, y_0) mit $p(x_0, y_0) = 0$, $|x_0| < X$ und $|y_0| < Y$ finden.

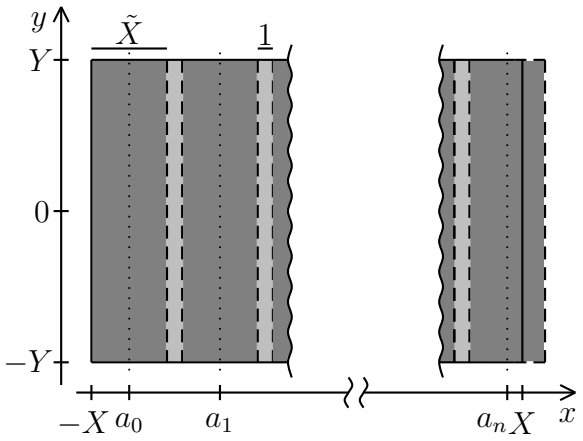
Beweis. Zuerst wählen wir Schranken X und Y, die den Anforderungen des Korollars genügen. Daraus berechnen wir

$$\tilde{X} = \lfloor 2^{-5-\frac{2}{\delta}-14\delta} X \rfloor$$

Ist das so berechnete $\tilde{X}$ eine ungerade Zahl wählen wir stattdessen

$$\tilde{X} = \lfloor 2^{-5-\frac{2}{\delta}-14\delta} X \rfloor - 1$$

Mit Hilfe von $\tilde{X}$ legen wir auf dem Bereich $D_{X,Y}$ mehrere kleinere Teilbereiche fest.



Die einzelnen Teilbereiche haben untereinander einen Abstand von 1, da in den Zwischenräumen keine ganzzahlige Nullstelle des Polynoms liegt. Die Mittelpunkte der Teilbereiche sind durch

$$a_i = -X + \frac{1}{2}\tilde{X} + i(\tilde{X}+1) \qquad i = 0, 1, \ldots$$

gegeben, wobei $a_i \leq X$ gilt. Für alle a_i berechnen wir jeweils das Polynom $p_a(x, y)$ und mittels des Basisverfahrens dessen Nullstellen auf dem Bereich $D_{\tilde{X},Y}$. Dabei verwenden wir jeweils den Parameter $\varepsilon = 1/\log W_a(\tilde{X}, Y)$. Aus den so gewonnenen Nullstellen $(x_0^{(a)}, y_0)$ des verschobenen Polynoms berechnen wir die Nullstellen $(x_0 - a, y_0)$ des Polynoms $p(x, y)$.

Dass die Voraussetzung (1) des Basisverfahrens erfüllt ist, zeigt die folgenden Berechnung. Auf Grund von

$$\frac{\tilde{X}}{X} \leq 2^{-5-\frac{2}{\delta}-14\delta}$$

gilt für das Produkt $\tilde{X}Y$

$$\begin{aligned}
\tilde{X}Y &= \frac{\tilde{X}}{X} \cdot XY \\
&< \frac{\tilde{X}}{X} \cdot W^{\frac{2}{3\delta}} \\
&\leq \frac{\tilde{X}}{X} \cdot \left[2^{\delta+1} \left(\frac{\tilde{X}}{X} \right)^{-\delta} W_a \right]^{\frac{2}{3\delta}} \\
&= \frac{\tilde{X}}{X} \cdot 2^{\frac{2}{3}+\frac{2}{3\delta}} \left(\frac{\tilde{X}}{X} \right)^{-\frac{2}{3}} \cdot W_a^{\frac{2}{3\delta}} \\
&= 2^{\frac{2}{3}+\frac{2}{3\delta}} \left(\frac{\tilde{X}}{X} \right)^{\frac{1}{3}} \cdot W_a^{\frac{2}{3\delta}} \\
&\leq 2^{\frac{2}{3}+\frac{2}{3\delta}} \cdot 2^{-\frac{5}{3}-\frac{2}{3\delta}-\frac{14}{3}\delta} \cdot W_a^{\frac{2}{3\delta}} \\
&= \frac{1}{2} W_a^{\frac{2}{3\delta}} \cdot 2^{-\frac{14}{3}\delta}
\end{aligned}$$

Ersetzen wir den Faktor $\frac{1}{2}$ durch

$$\frac{1}{2} = W_a^{-\frac{1}{\log_2 W_a}} = W_a^{-\varepsilon}$$

erhalten wir die Ungleichung

$$\tilde{X}Y < W_a^{\frac{2}{3\delta}-\varepsilon} \cdot 2^{-\frac{14}{3}\delta}$$

Diese entspricht genau der Voraussetzung für das Basisverfahren.

Es bleibt nun noch zu zeigen, dass unser Verfahren die Anforderung des Korollars an die Laufzeit einhält. Eine einzige Ausführung des Basisverfahrens hat gemäß (2) eine Laufzeit von

$$\begin{aligned}
\mathcal{O}((\log W_a)^{e_1} \cdot \delta^{e_2} \cdot (1/\varepsilon)^{e_3}) &= \mathcal{O}((\log W_a)^{e_1} \cdot \delta^{e_2} \cdot (\log W_a)^{e_3}) \\
&= \mathcal{O}((\log W_a)^{e_1+e_3} \cdot \delta^{e_2}) \\
&= \mathcal{O}((\delta+1)^{e_1+e_3} (\log W)^{e_1+e_3} \cdot \delta^{e_2}) \\
&= \mathcal{O}((\log W)^{e_4} \cdot \delta^{e_5})
\end{aligned}$$

ist also polynomiell in $(\log W, \delta)$. Die, zur Transformation der Nullstellen und Berechnung des verschobenen Polynoms benötigte Zeit, kann gegenüber der Laufzeit des Basisverfahrens vernachlässigt werden. Insgesamt wird das Basisverfahren weniger als $(2 \cdot 2^{5+\frac{2}{\delta}+14\delta} + 4)$-mal ausgeführt. Aus diesen Wiederholung resultiert damit eine Gesamtlaufzeit von

$$\mathcal{O}((\log W)^{e_1} \cdot (2^{\delta})^{e_2})$$

für das modifizierte Verfahren. □

7 Offene Probleme

Wir haben einen Polynomialzeit-Algorithmus entwickelt, der Nullstellen eines bivariaten Polynoms über den ganzen Zahlen berechnet und dabei die Anforderungen des Korollars von Coppersmith erfüllt. Der Algorithmus ist jedoch nur für kleine δ praktisch effizient, da in der Laufzeit hohe Konstanten auftreten. Eine mögliche Ursache dafür könnte in den teilweise großzügigen Abschätzungen dieser Arbeit liegen. Indem man diese weiter verbessert, ist es vielleicht möglich die Konstanten abzusenken und damit das Verfahren auch für Polynome höheren Grades anzuwenden.

Literatur

[1] Don Coppersmith, *Small Solutions to Polynomial Equations, and Low Exponent RSA Vulnerabilities*, Journal of Cryptology **10** (1997), 233–260.

[2] Yair Frankel, Dan Boneh, Glenn Durfee, *Exposing an RSA Private Key Given a Small Fraction of its Bits*, Full version of the work from Asiacrypt **98**.

[3] Alexander May, Johannes Blömer, *A Generalized Wiener Attack on RSA*, Practice and Theory in Public Key Cryptography (PKC 2004), Lecture Notes in Computer Science, Springer-Verlag **2947** (2004), 1–13.

[4] Werner Schindler, *A timing attack against RSA with the chinese remainder theorem*, CHES 2000 (2000), 109–124.