2.10 Weitere Angriffe

Einige weitere Angriffsansätze werden hier nur überblicksartig erwähnt; für eine ausführlichere Behandlung sei auf den in der Einleitung zitierten Artikel von D. Boneh verwiesen:

1. **Kleine private Exponenten.** M. Wiener hat eine Möglichkeit entdeckt, mit Hilfe eines Kettenbruch-Algorithmus den privaten Schlüssel d aus dem öffentlichen Schlüssel (n, e) effizient zu bestimmen, wenn $d < \frac{1}{3} \cdot \sqrt[4]{n}$.

2. **Abhängige Klartexte** nach Franklin/ Reiter. Gibt es einen affinen Zusammenhang $a_2 = sa_1 + t$ zwischen zwei verschiedenen Klartexten a_1 und a_2 mit bekannten Koeffizienten s und $t \neq 0$, so sind die Klartexte effizient aus dem öffentlichen Schlüssel (n, e), den Koeffizienten s und t sowie den zugehörigen Geheimtexten bestimmbar. Coppersmith hat gezeigt, wie man einen solchen affinen Zusammenhang antreffen kann, wenn a_1 und a_2 aus demselben Klartext durch unterschiedliches „Padding“ entstehen.

3. **Partielles Leck** nach Boneh/ Durfee/ Frankel/ Coppersmith. Falls das letzte Viertel der Bits von einer der Zahlen d (dem privaten Schlüssel) p oder q (den Primfaktoren des Moduls) bekannt sind, ist n effizient faktorisierbar.

4. **Timing- und Power-Attacken** nach Kocher. Hier wird der Prozessor beim Verschlüsseln beobachtet und aus seinem Zeitbedarf oder Stromverbrauch auf die Bits des geheimen Schlüssels geschlossen; dieser Angriff beruht darauf, dass diese Werte in den Ressourcenverbrauch des binären Potenzalgorithmus eingehen.

5. **Differenzielle Fehleranalyse** nach Shamir u. a. Hier wird der Prozessor (etwa auf einer Chipkarte) ein wenig über den spezifizierten Bereich seines einwandfreien Funktionierens gebracht – etwa durch Verbiegen, Erwärmen, Bestrahlen. Aus einzelnen Bitfehlern werden statistische Aussagen über die internen Parameter gewonnen.

Eine Reihe weiterer Angriffe sind bekannt, die sich nicht gegen das RSA-Verfahren direkt richten, sondern gegen Fehler bei der Implementation, Verwendung in kryptographischen Protokollen, Einbindung in eine Systemumgebung u. ä.

Dass ein RSA-Verfahren mit mehr als zwei Primfaktoren nicht schwächer, gegen manche Angriffe sogar resistenter ist, wird plausibel gemacht in:

- M. Jason Hinek, Mo King Low, Edlyn Teske: On some attacks on multi-prime RSA. SAC 2002, 385–404.