6.4 Physikalische Komplexität

Der unmittelbar einleuchtende Ansatz zur Beurteilung der Komplexität von Algorithmen ist die Zählung von Basisoperationen, wie sie auf einem handelsüblichen Prozessor ausgeführt werden, oder genauer von Taktzyklen. Dies führt zu konkreten Komplexitätsaussagen der Art: „Zur Berechnung von ... sind mindestens (z. B.) 10^{80} der folgenden Rechenschritte nötig: ... ". Hier würde man z. B. elementare arithmetische Operationen zählen (Additionen, Multiplikationen, ...) und berücksichtigen, wie groß die Wortlänge eines gegebenen Prozessors ist (z. B. 32 Bit) und wieviele Taktzyklen eine solche Operation auf einem gegebenen Prozessor in Anspruch nimmt. [Diese Zahl ist auf modernen Prozessoren mit Pipeline-Architektur allerdings nicht immer wohldefiniert.]

Derartige Aussagen sind natürlich für konkret gegebene Algorithmen möglich und führen oft auf interessante mathematische Probleme, wie D. Knuth in seinen Büchern immer wieder vorgeführt hat. Ergebnisse, die aussagen, wieviele Rechenschritte *jeder* Algorithmus zur Lösung eines bestimmten Problems mindestens enthalten muss, hat leider keine Art von Komplexitätstheorie zu bieten, außer für ganz einfache Probleme wie die Auswertung eines Polynoms an einer Stelle. Mit solchen Aussagen könnte man wirkliche Sicherheitsaussagen für Verschlüsselungsverfahren mathematisch beweisen, ohne auf unbewiesene Vermutungen und heuristische Argumente zurückgreifen zu müssen.

Dazu würde man auf physikalische Schranken zurückgreifen können, die sagen, welche Ressourcen Rechner höchstens zur Verfügung haben. Eine bekannte Abschätzung dieser Art sieht so aus (nach Louis K. Scheffer in `sci.crypt`):

- Es gibt höchstens 10^{90} Elementarteilchen im Universum – das ist eine Schranke für Zahl der möglichen CPUs –,
- Es braucht mindestens 10^{-35} Sekunden, um ein Elementarteilchen mit Lichtgeschwindigkeit zu durchqueren – das ist eine Zeitschranke für eine Operation –,
- Das Universum hat eine Lebensdauer von höchstens 10^{18} Sekunden ($\approx 30 \times 10^9$ Jahre) – das ist eine Schranke für die verfügbare Zeit.

Daraus folgt, dass höchstens $10^{143} \approx 2^{475}$ Operationen in diesem Universum möglich sind. Insbesondere sind 500-Bit-Schlüssel sicher vor vollständiger Suche ...

> ... until such time as computers are built from something other than matter, and occupy something other than space. (Paul Ciszek)

Diese Sicherheitsschranke gilt aber nur für den einen Algorithmus „vollständige Suche“; sie sagt nichts über die Sicherheit auch nur eines einzigen kryptographischen Verfahrens!

Natürlich ist eine realistische obere Schranke um viele Größenordnungen kleiner.

Zum Vergleich noch ein paar kryptologisch relevante Größen:

Sekunden/Jahr	3×10^7
CPU-Zyklen/Jahr auf 1-GHz-Rechner	3.2×10^{16}
Alter des Universums in Jahren	10^{10}
CPU-Zyklen seither (1 GHz)	3.2×10^{26}
Atome in der Erde	10^{51}
Elektronen im Universum	8.37×10^{77}
ASCII-Ketten der Länge 8 (95^8)	6.6×10^{15}
Binärketten der Länge 56 (2^{56})	7.2×10^{16}
Binärketten der Länge 80	1.2×10^{24}
Binärketten der Länge 128	3.4×10^{38}
Binärketten der Länge 256	1.2×10^{77}
75-stellige Primzahlen (ca 250 Bit)	5.2×10^{72}