5.4 Die Erfolgswahrscheinlichkeit

Die Überlegung aus Abschnitt 5.2 sieht im allgemeinen Rahmen von Abschnitt 5.1 genauso aus und liefert eine zufriedenstellende Antwort auf die dortige Frage 2:

Hauptsatz 1 (Formel von MATSUI**)** *Sei (α, β) eine lineare Relation mit Wahrscheinlichkeit $p = p_F(\alpha, \beta)$ und Potenzial $\lambda = \lambda_F(\alpha, \beta)$ für die Bitblock-Chiffre $F : \mathbb{F}_2^n \times \mathbb{F}_2^l \longrightarrow \mathbb{F}_2^n$. Dann ist die Erfolgswahrscheinlichkeit $P_{\alpha\beta N}$ der linearen Kryptoanalyse mit N bekannten Klartexten gerade die kumulierte Wahrscheinlichkeit $p_N^{(s)}$ der hypergeometrischen Verteilung zu den Parametern 2^n, $s = 2^n \cdot \max\{p, 1-p\}$ und N. Ist $p \approx \frac{1}{2}$, $N \ll 2^n$ und N nicht zu klein, so*

$$P_{\alpha\beta N} \approx \frac{1}{\sqrt{2\pi}} \cdot \int_{-\infty}^{\sqrt{N\lambda}} e^{-t^2/2} dt.$$

Für die exakte Verteilung haben wir die Bedingung

$$p_{\alpha\beta N} = 1, \quad \text{wenn } N > 2^{n+1}(1 - p_1).$$

Diese nützt für $p \approx \frac{1}{2}$ nichts – der Aufwand für die lineare Kryptoanalyse ist genauso groß wie der für die Exhaustion. Verzichtet man aber auf die hundertprozentige Gewissheit, so ergibt die Näherungsformel zusammen mit den bekannten Regeln für die Normalverteilung die Tabelle

$N\lambda$	1	2	3	4	...	8	9
$P_{\alpha\beta N}$	84.1%	92.1%	95.8%	97.7%	...	99.8%	99.9%

D. h., um eine Erfolgswahrscheinlichkeit von 97.7% zu erreichen, braucht man $N \approx \frac{4}{\lambda}$ bekannte Klartexte.

Zahlenbeispiel für DES: Das höchste Potenzial einer linearen Relation ist $\lambda \approx (3 \cdot 2^{-24})^2$ (siehe später), die entsprechende Wahrscheinlichkeit $p \approx \frac{1}{2} - 3 \cdot 2^{-25}$. Für eine Erfolgswahrscheinlichkeit von 97.7% benötigt man also $N\lambda \approx 4$, also

$$N \approx \frac{4}{\lambda} \approx \frac{4 \cdot 2^{48}}{3^2} \approx 2^{47}$$

bekannte Klartexte. Damit hat man dann *ein* Schlüsselbit mit hoher Wahrscheinlichkeit bestimmt.

> Leichte Verbesserungen: Mit einer linearen Relation für die Runden 2 bis 15 und einer vollständigen Suche über die relevanten Schlüsselbits der Runden 1 und 16 konnte MATSUI die Anzahl der benötigten Klartexte auf 2^{43} drücken; durch gleichzeitiges Betrachten mehrerer linearer Relationen konnte er ferner die Anzahl der gewonnenen Schlüsselbits auf 14 erhöhen. Es bleibt die vollständige Suche nach den übrigen 42 Schlüsselbits, die auf einem PC nur noch wenige Sekunden dauert.

Dies ist der effizienteste bekannte Angriff auf das DES-Verfahren; die Anzahl der benötigten Klartexte ist allerdings immer noch so groß, daß dieser Angriff kaum als realistische Gefahr eingestuft werden kann. Dennoch offenbart er eine leichte Schwäche, die beim Design des DES übersehen wurde. Wir werden später sehen, dass die Stabilität des DES gegen differenzielle Kryptoanalyse deutlich besser ist; diese Angriffsmöglichkeit war ja, wie heute bekannt ist, beim Design berücksichtigt worden.