

1 Die Idee der linearen Kryptoanalyse

Sei

$$F: \mathbb{F}_2^n \times \mathbb{F}_2^l \longrightarrow \mathbb{F}_2^n$$

eine Bitblock-Chiffre. Wir stellen uns die Argumente von F als Klartexte $a \in \mathbb{F}_2^n$ und Schlüssel $k \in \mathbb{F}_2^l$, die Werte von F als Geheimtexte $c \in \mathbb{F}_2^n$ vor. Dann kann man zu zwei Linearformen

$$\alpha: \mathbb{F}_2^n \times \mathbb{F}_2^l \longrightarrow \mathbb{F}_2, \quad \text{und} \quad \beta: \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$$

die Wahrscheinlichkeit der linearen Relation (α, β) beziehungsweise ihr Potenzial betrachten:

$$p_F(\alpha, \beta) = \frac{1}{2^{n+l}} \cdot \#\{(a, k, c) \in \mathbb{F}_2^n \times \mathbb{F}_2^l \times \mathbb{F}_2^n \mid c = F(a, k), \alpha(a, k) = \beta(c)\},$$
$$\lambda_F(\alpha, \beta) = (2p_F(\alpha, \beta) - 1)^2 = \frac{1}{2^{2n+2l}} \cdot \hat{\vartheta}_F(\alpha, \beta),$$

wobei in der Notation nicht zwischen einer Linearform und dem zugehörigen Vektor unterschieden wird. Zerlegt man $\alpha(a, k)$ in die Summe $\alpha'(a) + \gamma(k)$ – und schreibt dann statt α' einfach in neuer Bedeutung α –, so kann man sagen, dass $p_F((\alpha, \gamma), \beta)$ die Wahrscheinlichkeit dafür angibt, dass bei bekanntem Klartext a die lineare Relation

$$\gamma(k) = \alpha(a) + \beta(c)$$

für die Schlüsselbits k_{i_1}, \dots, k_{i_r} gilt, wenn $I = (i_1, \dots, i_r)$ die Indexmenge ist, die der Linearform γ entspricht. Dabei ist $\gamma(k) = k_{i_1} + \dots + k_{i_r}$ ein einzelnes Bit, das die durch I definierte Summe einiger Bits des Schlüssels k darstellt. Das Potenzial $\lambda_F((\alpha, \gamma), \beta)$ misst die Abweichung der Wahrscheinlichkeit vom Wert $\frac{1}{2}$, denn eine Wahrscheinlichkeit $< \frac{1}{2}$ ist genauso gut wie eine $> \frac{1}{2}$: Sie sagt, dass die Relation

$$\gamma(k) = \alpha(a) + \beta(c) + 1$$

überzufällig oft gilt.

Daraus leitet man folgenden Algorithmus für die Schätzung von $\gamma(k)$ ab:

1. [**Sammelphase**] Man sammelt N Klartext-Geheimtextpaare $(a_1, c_1), \dots, (a_N, c_N)$.
2. [**Auszählung**] Man bestimmt die Anzahl

$$t_0 := \#\{i = 1, \dots, N \mid \alpha(a) + \beta(c) = 0\}.$$

3. [**Mehrheitsentscheidung**] aufgrund von t_0 :

- Ist $t_0 > \frac{N}{2}$, schätzt man $\gamma(k) = 0$.

- Ist $t_0 = \frac{N}{2}$, „randomisiert“ man die Entscheidung, d. h., man entscheidet sich zufällig für 0 oder 1, jeweils mit Wahrscheinlichkeit $\frac{1}{2}$.
- Ist $t_0 < \frac{N}{2}$, schätzt man $\gamma(k) = 1$.

Wenn man ein lineare Relation mit hinreichend hohem Potenzial erwischt hat, wird die Erfolgswahrscheinlichkeit dieses Verfahrens bei hinreichend großem N hinreichend gut sein.

Findet man mehrere solche lineare Relationen mit hinreichender Gewissheit, so hat man den Schlüsselraum auf einen Unter-Vektorraum eingeschränkt und kann über diesen eine Exhaustion versuchen. Das ist die Grundidee der linearen Kryptoanalyse – es gibt je nach dem konkreten Aufbau einer Chiffre verschiedene Varianten, wie in den folgenden Abschnitten deutlich wird.

Als theoretisches Ergebnis aus der Analyse einer Chiffre erhält man dadurch einen Zusammenhang zwischen der Menge von benötigtem Klartext und der Erfolgswahrscheinlichkeit oder auch der Dimension des übriggebliebenen Suchraums.

Damit das Verfahren anwendbar ist, sind folgende Fragen zu klären:

1. Wie findet man lineare Relationen von möglichst großem Potenzial?
Diese Fragen kann man unterteilen in die Teilfragen:
 - (a) Wie findet man bei einer iterierten Bitblock-Chiffre brauchbare lineare Relationen für die Rundenfunktion?
 - (b) Wie setzt man diese über die Runden hinweg zu linearen Relationen für die ganze Chiffre zusammen, so dass Aussagen über Schlüsselbits resultieren?
 - (c) Wie bestimmt man die Wahrscheinlichkeit einer zusammengesetzten linearen Relation für die ganze Chiffre aus der für die einzelnen Runden?
2. Wie hängt die Erfolgswahrscheinlichkeit von der Zahl N der bekannten Klartext-Blöcke ab?

Die Antwort auf die erste Frage heißt: Aus dem linearen Profil, also durch FOURIER-Analyse der Rundenfunktion. Die weiteren Fragen führen zur Untersuchung von „linearen Pfaden“ und „linearen Hüllen“ und der Kumulation von Wahrscheinlichkeiten.