



2. Übungsblatt - Lösungshinweise

ÜBUNGEN

G1 (Affin-Lineare Chiffre).

Wir betrachten die affin-lineare Chiffre mit Verschlüsselungsfunktion $c = A * p + \mathbf{b}$ mit $A \in \mathbb{Z}_7^{(2,2)}$ und $\mathbf{b} \in \mathbb{Z}_7^2$. Der Klartext 12 34 65 wird im ECB-Modus zum Chiffretext 55 04 02 verschlüsselt. Bestimmen sie A und \mathbf{b} , sowie die Entschlüsselungsfunktion.

Lösung. Um die Abhängigkeit mit \mathbf{b} zu eliminieren, bilden wir zuerst Differenzen zwischen Klartextpaaren und Chiffretextpaaren. Es gilt: $c_1 = A * p_1 + \mathbf{b}$ und $c_2 = A * p_2 + \mathbf{b}$. Damit gilt für die Differenz: $c_1 - c_2 = (A * p_1 + \mathbf{b}) - (A * p_2 + \mathbf{b}) = (A * p_1) - (A * p_2) = A * (p_1 - p_2)$. Ebenso $c_2 - c_3 = A * (p_2 - p_3)$. Wir benutzen die Differenzen als Spaltenvektoren für eine Matrix, und erhalten so

$$P = \begin{pmatrix} 5 & 4 \\ 5 & 6 \end{pmatrix}$$

und

$$C = \begin{pmatrix} 5 & 0 \\ 1 & 2 \end{pmatrix}$$

Nun gilt $AP = C$. Durch Multiplikation mit P^{-1} erhalten wir: $A = CP^{-1}$ mit

$$P^{-1} = \begin{pmatrix} 2 & 1 \\ 3 & 4 \end{pmatrix}$$

Damit ist die geheime Matrix

$$A = \begin{pmatrix} 3 & 5 \\ 1 & 2 \end{pmatrix}$$

Als nächste bestimmen wir \mathbf{b} . Wir wissen dass $A * p_1 + b = c_1$ gilt, und damit gilt

$$b = c_1 - A * p_1 = \begin{pmatrix} 6 \\ 0 \end{pmatrix}$$

Die Entschlüsselungsfunktion ist somit:

$$p = \begin{pmatrix} 2 & 2 \\ 6 & 3 \end{pmatrix} \left(c - \begin{pmatrix} 6 \\ 0 \end{pmatrix} \right)$$

G2 (Mehrfachverschlüsselung).

Unter Mehrfachverschlüsselung verstehen wir folgendes: Ein Klartext p wird unter Verwendung des Schlüssels K_1 zum Schlüsseltext $c_1 = E_{K_1}(p)$ verschlüsselt. Dann wird c_1 unter Verwendung eines 2. Schlüssels K_2 zum Chiffretext $c_2 = E_{K_2}(c_1) = E_{K_2}(E_{K_1}(p))$ verschlüsselt.

- Beschreiben sie dieses Verschlüsselungssystem formal. Was sind Klartextrraum (\mathcal{P}), Chiffretextraum (\mathcal{C}), Schlüsselraum (\mathcal{K}), Menge der Verschlüsselungsfunktionen (\mathcal{E}) und Menge der Entschlüsselungsfunktionen (\mathcal{D})?

Wir bezeichnen mit $'$, das ursprüngliche Verschlüsselungssystem. \mathcal{P} und \mathcal{C} bleiben unverändert, also $\mathcal{P} = \mathcal{P}'$ und $\mathcal{C} = \mathcal{C}'$.

Der Schlüsselraum besteht jetzt aus 2 Schlüsseln des ursprünglichen Systems, also $\mathcal{K} = \mathcal{K}' \times \mathcal{K}'$, wobei wir die einzelnen Teilschlüssel von \mathcal{K} mit \mathcal{K}_1 und \mathcal{K}_2 bezeichnen werden.

Die Verschlüsselungsfunktionen sind: $\mathcal{E} = \{E_{\mathcal{K}}(m) = E'_{\mathcal{K}_2}(E'_{\mathcal{K}_1}(m))\}$ mit $\mathcal{K} = (\mathcal{K}_1, \mathcal{K}_2)$.

Entschlüsselungsfunktionen: $\mathcal{D} = \{D_{\mathcal{K}}(c) = D'_{\mathcal{K}_1}(D'_{\mathcal{K}_2}(c))\}$ mit $\mathcal{K} = (\mathcal{K}_1, \mathcal{K}_2)$.

- Erhöht sich die Sicherheit einer affin-linearen Blockchiffre bei Mehrfachverschlüsselung?

Nein, es gilt $c = A_2 * (A_1 * p + \mathbf{b}_1) + \mathbf{b}_2 = A_2 * A_1 * p + (A_2 * \mathbf{b}_1 + \mathbf{b}_2) = \tilde{A} * p + \tilde{\mathbf{b}}$. Auch hier ist die Mehrfachverschlüsselung mit Schlüsseln \mathcal{K}_1 und \mathcal{K}_2 äquivalent zu der Verschlüsselung mit einem einzigen Schlüssel $\tilde{\mathcal{K}}$.

G3 (Bitdifferenzen).

2 Klartextblöcke p_1 und p_2 werden mit einer affin-linearen Blockchiffre mit Blocklänge 3 mit dem selben Schlüssel verschlüsselt ($\Sigma = \{0, 1\}$). Die Klartexte unterscheiden sich an genau an einer Position. An wie vielen Positionen unterscheiden sich die beiden Chiffretexte minimal und maximal? Lösen sie das Problem zuerst für Blocklänge 3. Konstruieren sie also entsprechende Klartexte und den Schlüssel. Verallgemeinern sie Ihre Lösung dann für beliebige Blocklängen.

Lösung. Die Differenz wirkt sich minimal auf ein Bit der Ausgabe auf, und maximal auf alle. Dass sich eine Änderung in der Eingabe auf kein Bit der Ausgabe auswirkt, kann nicht passieren, da die Abbildung invertierbar sein muss. Für den Maximalfall kann man einfach ein Beispiel konstruieren.

Wir wählen A wie die Identität, nur die erste Spalte der Matrix besteht nur aus 1-Einträgen. In diesem Fall ist die Matrix sogar invers zu sich selbst, also $A^2 = I$. Wie man leicht sehen kann, erzeugt Multiplikation mit $(0, \dots, 0)$ den 0-Vektor, Multiplikation mit $(1, 0, 0, \dots, 0)$ den 1-Vektor.

G4 (Permutationen).

Wir betrachten die Menge aller möglichen Permutationen der Menge $\{0, 1\}^2$.

- Wie viele dieser Permutationen sind Bitpermutationen, d. h. sie vertauschen nur die Positionen der Bits?

Wir können die Bits entweder vertauschen oder nicht, damit gibt es genau 2 Bitpermutationen.

- Wie viele dieser Permutationen sind linear?

Es gibt insgesamt 6 verschiedene invertierbare Matrizen in $\mathbb{Z}_2^{(2,2)}$. Zwei dieser Matrizen sind Permutationsmatrix, die restlichen 4 Matrizen haben alle Einträge auf 1 gesetzt, bis auf jeweils eine Position, die dann 0 ist.

- Wie viele dieser Permutationen sind affin-linear?

Alle der Permutationen sind affin-linear. Wir haben insgesamt 6 verschiedene Möglichkeiten, die Matrix invertierbar zu wählen. Jede dieser 6 Möglichkeiten können wir mit einem Vektor \mathbf{b} kombinieren, für den es 4 Möglichkeiten gibt. Zu zeigen ist jetzt noch, dass alle Permutationen wirklich verschieden sind.

Alle linearen Permutationen sind auf jeden Fall 0-erhaltend. Angenommen es gäbe 2 Funktionen $A * x + b$ und $A' * x + b'$, mit unterschiedlichen b' oder A' , die aber die selbe Permutation beschreiben. Wir ziehen b von beiden Permutationen ab, und erhalten $A' * x + (b' - b)$ und $A * x$. Da $A * x$ linear ist, müsste ebenfalls auch $A' * x + (b' - b)$ 0-erhalten sein, und damit $b' - b = 0$ und damit $b' = b$ gelten. Damit können sich die Permutationen nur noch in A und A' unterscheiden. Wir betrachten nun weiter $A * x$ und $A' * x$: Da beide Funktionen nun linear sind, sind A und A' gleich und durch die Funktionswerte bereits eindeutig bestimmt.

- Wie viele bleiben übrig?

Keine.

G5 (*Abschätzung Permutationen*).

Schätzen sie die Anzahl der affin-linearen Permutationen von $\{0, 1\}^n$ möglichst gut ab. Tragen Sie in einem Graphen die Anzahl und die Gesamtzahl der Permutationen als Funktion in Abhängigkeit von n auf.

Lösung. Es gibt insgesamt $(2^n)!$ mögliche Permutationen, aber maximal 2^{n-n} mögliche Matrizen und 2^n mögliche Vektoren. Davon müssen noch nicht invertierbare Matrizen abgezogen werden. Insgesamt kann es damit nicht mehr als $2^{n^2+n} = 2^{n(n+1)}$ affin-lineare Abbildungen geben.

Bereits ab $n = 5$ ist die Wahrscheinlichkeit, dass eine zufällige Permutation affin-linear ist weniger als 10^{-25} .

Man kann auch eine exakte Formel finden, es gibt genau:

$$2^{n^2} \prod_{i=1}^n \left(1 - \frac{1}{2^i}\right)$$

invertierbare Matrizen in $\mathbb{Z}_2^{(n,n)}$.