Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Elena Kirshanova, Ilya Ozerov

Präsenzübungen zur Vorlesung

Kryptanalyse

SS 2014

Blatt 4 / 12. Mai 2014

AUFGABE 1:

Wir betrachten den Repräsentationsangriff auf Subset Sum, d.h. zu finden ist $I \subseteq \{1, \ldots, n\}$ mit $|I| = \frac{n}{2}$ und $\sum_{i \in I} a_i = S$. Eine Möglichkeit die Anzahl der Repräsentationen zu erhöhen ist zusätzlich mit negierten Gewichten zu arbeiten, wodurch auch Elemente $i \notin I$ verschiedene Repräsentationsmöglichkeiten haben. Wir erhalten die Gleichung

$$\sum_{i \in I_1} a_i - \sum_{i \in J_1} a_i = S - \left(\sum_{i \in I_2} a_i - \sum_{i \in J_2} a_i \right)$$

mit $I_1, I_2, J_1, J_2 \subseteq \{1, \ldots, n\}$, $I_1 \cap J_1 = \emptyset$, $I_2 \cap J_2 = \emptyset$, $|I_1| = |I_2| = \frac{n+m}{4}$, $|J_1| = |J_2| = \frac{m}{4}$ für $m, n \in 4\mathbb{N}$. Sei nun $S = \sum_{i \in I} a_i$ mit $I \subseteq \{1, \ldots, n\}$ und $|I| = \frac{n}{2}$. Wie viele Repräsentationen $S = S_1 + S_2$ mit $S_1 = \sum_{i \in I_1} a_i - \sum_{i \in J_1} a_i$ und $S_2 = \sum_{i \in I_2} a_i - \sum_{i \in J_2} a_i$ existieren?

AUFGABE 2:

Wir betrachten nun eine Variante des Subset Sum Problems. Sei $n \in 16\mathbb{N}$. Zu finden ist $I \subseteq \{1, \ldots, n\}$ mit $|I| = \frac{n}{4}$ und $\sum_{i \in I} a_i = S \bmod N$, d.h. die Anzahl der Aufsummierten a_i's ist $\frac{n}{4}$ statt $\frac{n}{2}$. Zudem gilt die Gleichung modulo $N = pq$ mit $p = \Theta(\binom{n/4}{n/8})$. Beschreiben Sie einen Repräsentationsangriff, der das Problem in $\widetilde{\mathcal{O}}(\binom{n}{n/8} / \binom{n/4}{n/8})$ löst. Zeigen Sie Laufzeit und Korrektheit. Verwenden Sie, dass $\binom{n/2}{n/16} < \binom{n}{n/8} / \binom{n/4}{n/8}$.

AUFGABE 3:

Der Algorithmus von Stern für das Syndrom-Dekodierproblem kann mit Hilfe der Repräsentationstechnik verbessert werden. Wir betrachten das folgende Problem mit $t \in \mathbb{N}$, $n \in 8\mathbb{N}$. Gegeben sind $a_1, \ldots, a_n, s \in \mathbb{F}_2^t$. Gesucht ist ein $I \subseteq \{1, \ldots, n\}$ mit $|I| = \frac{n}{4}$ und $\sum_{i \in I} a_i = s$. Seien $I_1, I_2 \subseteq \{1, \ldots, n\}, |I_1| = |I_2| = \frac{n}{8}$. Wie viele Repräsentationen $s = s_1 + s_2$ mit $s_1 = \sum_{i \in I_1} a_i$ und $s_2 = \sum_{i \in I_2} a_i$ existieren?