RUHR UNIVERSITÄT BOCHUM

Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Elena Kirshanova

Präsenzübungen zur Vorlesung

Kryptanalyse I

SS 2015

Blatt 4 / 25 Juni 2015

Aufgabe 1:
The BKW algorithm.
In the BKW algorithm after performing $\widetilde{\mathcal{O}}(2^{\frac{n}{\log n}})$ steps, we receive a sample

$$\langle \mathbf{u}_1, \mathbf{s} \rangle + e = s_1 + e = l,$$

where $\Pr[e = 1] = \frac{1}{2} + \frac{1}{2}(1-2p)^{2^{a-1}}$. How many such samples do you need to deduce on the value s_1 with probability exponentially close to 1?
Hint. Use Hoeffding's inequality: Let $X_1, \ldots, X_n$ be independent $\{0,1\}$-valued random variables with $\Pr[X_i = 1] = p$. Let $X = \sum_{i=1}^{n} X_i$. Then

$$\Pr[|X - pn| \geq \gamma pn] \leq e^{-n\gamma^2}.$$

Aufgabe 2:
Representation technique for the subset sum over $\mathbb{F}_2^n$.
Given matrix $\mathbf{A} \in \mathbb{F}_2^{n \times n}$ and $\mathbf{s} \in \mathbb{F}_2^n$, find a linear combination $I, |I| = \frac{n}{2}$ of the columns of $\mathbf{A}$, s.t. $\sum_{i \in I} \mathbf{a}_i = \mathbf{s}$. Doing this in the MITM way, one splits the columns of $\mathbf{A}$ by half, creates two lists of linear combinations for each half and searches for a collision:

$$\sum_{i \in I_1} \mathbf{a}_i = \mathbf{s} - \sum_{i \in I_2} \mathbf{a}_i, \tag{1}$$

where $|I_1| = |I_2| = \frac{n}{4}, I_1 \cap I_2 = \emptyset$.

1. Assume now that we allow the sets I_1, I_2 to overlap. In other word, we take $I_1, I_2 \subseteq [1..n]$. How many representations R does Eq.(1) have? What will be the size of the resulting list $|L_1|$?

2. Taking into an account the number of representations R, we need to enumerate only an $1/R$-fraction of L_1. To do so, we impose an additional constraint on elements in the list L_1. Think why the following constraint will be appropriate:

$$L_1 = \{\mathbf{x} \in \mathbb{F}_2^n, wt(\mathbf{x}) = \tfrac{n}{4} : \mathbf{A}\mathbf{x} = [\mathbf{0}^{n/2} | \mathbf{x}'], \mathbf{x}' \in \mathbb{F}_2^{n/2}\}.$$

   What does the list L_2 look like?

3. Explain how to construct the list L_1 (equivalently, L_2) using an MITM approach. With this, estimate the size of L_1 and time needed to construct it. Conclude on the running time of the decoding.

Aufgabe 3:
Allowing -1's in the representations.
You're given a subset-sum instance: $a_1, \ldots, a_n, S$, s.t.

$$\sum_{i=1}^{n} \varepsilon_i a_i = S, \quad wt(\varepsilon) = \frac{n}{4}.$$

In the representation, we enumerate a $1/R$-fraction of the lists

$$L_1 = \{\sum_{i=1}^{n} \varepsilon_i a_i, wt(\varepsilon) = \tfrac{n}{8}\}$$
$$L_2 = \{S - \sum_{i=1}^{n} \varepsilon_i a_i, wt(\varepsilon) = \tfrac{n}{8}\}$$

What is the size of the lists $|L_1|, |L_2|$? How many representations R of the solution is there? How will the number of representations R change, if we take $wt(\epsilon) = \frac{n}{8} + \alpha \cdot n, \alpha \in (0, 1/8)$?