RUHR UNIVERSITÄT BOCHUM

RUB

Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Gottfried Herold, Philipp Wagner

Präsenzübungen zur Vorlesung

Kryptanalyse

WS 2012/2013

Blatt 10 / 18. Dezember 2012

AUFGABE 1:
Geben Sie eine Verallgemeinerung des k-Listen Algorithmus an, so dass man $x_i \in L_i$ findet mit

$$x_1 \oplus \ldots \oplus x_k = c$$

für beliebiges $c \in \{0,1\}^n$. Der Algorithmus sollte die gleiche Laufzeit $\tilde{\mathcal{O}}(k2^{\frac{n}{\log k+1}})$ haben. Begründen Sie kurz die Korrektheit.

AUFGABE 2:
Lösen Sie die folgenden 4-Listen Probleme:

(a)

$$\begin{aligned} L_1 &= \{1010, 0111, 0100\} \\ L_2 &= \{1110, 0010, 1011\} \\ L_3 &= \{1011, 0111, 0011\} \\ L_4 &= \{0011, 1111, 1001\} \end{aligned}$$

(b)

$$\begin{aligned} L_1 &= \{100111, 110101, 001101, 111001\} \\ L_2 &= \{011011, 100011, 011010, 100101\} \\ L_3 &= \{010010, 001011, 000110, 111101\} \\ L_4 &= \{001011, 111000, 001010, 101101\} \end{aligned}$$

AUFGABE 3:
Wir betrachten die inkrementelle Hashfunktion **AdHash** wie im Skript, d.h. eine Nachricht $x = (x_1, \ldots, x_k)$ wird gehasht als

$$H(x) = \sum_{i=1}^{k} h(i, x_i) \bmod 2^n \ .$$

Dabei wollen wir annehmen, dass sich h wie eine zufällige Funktion verhält und k fest gewählt ist.

Überlegen Sie sich einen Algorithmus, der für festes $k = 2^j$ eine Kollision, d.h. $x \neq y$ mit $H(x) = H(y)$, $x = (x_1, \ldots, x_k)$, $y = (y_1, \ldots, y_k)$ findet in Laufzeit $\widetilde{O}(k \cdot 2^{\frac{n}{j+2}})$.

AUFGABE 4:
Seien $L_1, \ldots, L_k$ Listen mit unabhängig uniformen Elementen aus $\{0,1\}^n$. Wir interessieren uns für k-Tupel $x_1, \ldots, x_k$ mit $x_i \in L_i$, $\sum x_i = 0$. Die Existenz wie vieler solcher k-Tupel erwarten wir?
Zeigen Sie, dass, wenn $|L_1| \cdot \ldots \cdot |L_k| = 2^n(\alpha + t)$, wobei $t = \omega(\alpha), t = \omega(1)$, es mit Wahrscheinlichkeit $1 - o(1)$ mindestens α solcher k-Tupel gibt.
Beachten Sie, dass α, k, t hier implizit (möglicherweise konstante) Funktionen von n sind und wir $n \to \infty$ betrachten.
Hinweis: Benutzen Sie die Tschebyschew-Ungleichung und zur Berechnung der Varianz dabei die Tatsache, dass $\mathbf{Var}(\sum X_i) = \sum \mathbf{Var}(X_i)$ für *paarweise* unabhängige X_i gilt.

Frohe Weihnachten und einen Guten Rutsch!