TIN 085 - Vybrané kapitoly z výpočetní složitosti I **zima 2006/2007**

3. domácí úlohy - kryptografické pseudonáhodné generátory

do 19. prosince 2006

1. Nechť $A \in \{0,1\}^n$ a $B \in \{0,1\}^{n\times(n+1)}$ jsou vybrány náhodně. Ukažte, že pravděpodobnost, že $f(A,B) = (\sum_{i=1}^n A_i \cdot B_i, B)$ má jednoznačný předobraz, lze sdola odhadnout konstantou nezávislou na n. Zde jsou jednotlivá B_i interpretována jako celá čísla daná svým binárním zápisem a suma je také přes celá čísla.

2. V následujícím je f funkce mapující $\{0,1\}^n \to \{0,1\}^n$.

   (a) Popište jednosměrnou permutaci f, jejíž první bit není skrytý vzhledem k f.

   (b) Nechť f je funkce počitatelná v polynomiálním čase. Ukažte, že pokud x_i se dá z $(f(x), i)$ předpovídat správně s pravděpodobností větší než $1 - \frac{1}{2n}$, pro $x \in \{0,1\}$ a $i \in \{1,\dots,n\}$ vybráno náhodně, pak f není jednosměrná.

   (c) Popiště funkci f počítatelnou v polynomiálním čase, která zcela jistě není jednosměrná, avšak takovou, že $b(x,y) = \sum x_i y_i$ je (dokazatelně) skrytý bit pro $f'(x,y) = (f(x), y)$.

3. Náhodné proměnné $X_1, X_2, \dots, X_n$ jež nabývají hodnot z množiny H jsou po k-nezávislé, pokud pro každou jejich k-tici $X_{i_1}, X_{i_2}, \dots, X_{i_k}$ a každou k-tici prvků $h_1, \dots, h_k \in H$, $Pr[X_{i_1} = h_1 \& X_{i_2} = h_2 \& \cdots \& X_{i_k} = h_k] = Pr[X_{i_1} = h_1] \cdot Pr[X = h_2] \cdots Pr[X_{i_k} = h_k]$. S užitím polynomů nad konečnými tělesy, sestrojte co nejmenší pravděpodobnostní prostor a definujte nad ním po k-nezávislé náhodné proměnné $X_1, X_2, \dots, X_n$ jež nabývají hodnot 0 a 1, každé s pravděpodobností 1/2.

4. *How to share a secret.* Představte si, že máte skupinu n bankovních úředníků a chcete mezi ně rozdělit kód k trezoru tak, aby libovolná skupina k z nich mohla kód společně zrekonstruovat, ale aby žádná skupina méně než k z nich kód zrekonstruovat nemohla a neměla by o něm žádnou informaci (to jest z jim dostupné informace by kód mohl být stále ještě cokoliv.) Vytvořte takové schéma. V prvním přiblížení tedy chceme funkci $f : \{1,\dots,N\} \times \{1,\dots,R\} \to \{1,\dots,N\}^n$ takovou, že z libovolných k složek $f(x,r)$ můžeme jednoznačně určit x, ale pokud známe pouze $k-1$ složek $f(x)$, x může být libovolné. Zde x je onen kód k trezoru a r je parametr, který bude zvolen náhodně a též bude utajen.