Kapitulli 4

Funksionet pseudo të rastësishme

Detyra për ushtrime

1. Le të jetë $E : \{0,1\}^k \times \{0,1\}^\ell \to \{0,1\}^\ell$ një PRF i sigurt. Shqyrtoni një familje permutacionesh $E' : \{0,1\}^k \times \{0,1\}^{2\ell} \to \{0,1\}^{2\ell}$ të përkufizuar me

   $$(\forall x, x' \in \{0,1\}^\ell) \quad E'_K(x \parallel x') = E_K(x) \parallel E_K(x \oplus x')$$

   Tregoni se E' nuk është një FPR i sigurt.

2. Shqyrtoni blok shifruesin vijues $E : \{0,1\}^3 \times \{0,1\}^2 \to \{0,1\}^2$ (Secili

Çelësi	0	1	2	3
0	0	1	2	3
1	3	0	1	2
2	2	3	0	1
3	1	2	3	0
4	0	3	2	1
5	1	0	3	2
6	2	1	0	3
7	3	2	1	0

   rresht ka vlerën e çelësit K dhe jep vlerat $E_K(x)$ për çdo x.) Llogaritni prp-përparësinë maksimale që mund ta ketë një kundërshtar

   - me një orakul pyetësor,
   - me dy orakul pyetësorë,
   - me katër orakul pyetësorë.

3. Le të jetë $F : \{0,1\}^k \times \{0,1\}^\ell \to \{0,1\}^\ell$ një FPR. Disenjoni një FPR $G : \{0,1\}^k \times \{0,1\}^\ell \to \{0,1\}^{2\ell}$ i cili është PRF-i sigurt përderisa F është i tillë.

4. Disenjoni një blok shifrues $E : \{0,1\}^k \times \{0,1\}^{128} \to \{0,1\}^{128}$ i cili është i sigurt (deri te një numër i madh pyetësorësh) kundrejt kundërshtarëve joadaptivë, por është i pasigurt (madje për dy pyetësorë) kundrejt një kundërshtari adaptiv.

5. Le të jetë $E : \{0,1\}^k \times \{0,1\}^\ell \to \{0,1\}^\ell$ një blok shifrues. *Kaskadë e dyfishtë* e E është blok shifruesi $E^{(2)} : \{0,1\}^{2k} \times \{0,1\}^\ell \to \{0,1\}^{2\ell}$ i përkufizuar me

$$E^{(2)}(K_1 \parallel K_2, x) = E(K_1, E(K_2, x))$$

për çdo $K_1, K_2 \in \{0,1\}^k$ dhe për çdo $x \in \{0,1\}^\ell$. Vërtetoni se në qoftë se E është PRF-i sigurt, atëherë i tillë është edhe $E^{(2)}$.

6. Le të jetë $F : \{0,1\}^k \times \{0,1\}^\ell \to \{0,1\}^\ell$ një familje funksionesh dhe le të jetë $r \geq 1$ numër i plotë. *Shifruesi i Feistel-it r-raundësh* i shqëruar me F është familja e funksioneve $F^{(r)} : \{0,1\}^{rk} \times \{0,1\}^{2\ell} \to \{0,1\}^{2\ell}$ i përkurizuar si në vijim për çdo $K_1, \ldots, K_r \in \{0,1\}^k$ dhe për çdo $x \in \{0,1\}^{2\ell}$:

---

function $F^{(r)}(K_1 \parallel \cdots \parallel K_r,\ x)$
  Parso x si $L_0 \parallel R_0$ me $|L_0| = |R_0| = \ell$
  for $i = 1, \ldots, r$ **do**
    $L_i \leftarrow R_{i-1}$
    $R_i \leftarrow F(K_i, R_{i-1}) \oplus L_{i-1}$
  end for
  return $L_r \parallel R_r$
end function

Vërtetoni se ekziston një kundërshtar A, i cili bën të shumtën dy orakul pyetësorë dhe me kompleksitet afërsisht sa dy kompjutime të F, i tillë që

$$\mathrm{Adv}^{prf}_{F^{(2)}}(A) = 1 - 2^{-\ell}.$$