Α31 ΚΡΥΠΤΟΓΡΑΦΙΑ
Φυλλάδιο ασκήσεων #3

Θεόδουλος Γαρεφαλάκης

23 Μαρτίου 2022

Για τις παρακάτω ασκήσεις, δείτε τον ορισμό 7.5 στη σελίδα 264 του βιβλίου Boneh-Shoup.

1. (Boneh-Shoup 7.16) Έστω πρώτος p και φυσικός ℓ.

   (α΄) Δείξτε ότι η $H_1 : \mathbb{Z}_p \times \mathbb{Z}_p^\ell \to \mathbb{Z}_p$ με τύπο $H_1(k, (a_1, \ldots, a_\ell)) = a_1 k^{\ell-1} + \cdots + a_{\ell-1}k + a_\ell$ είναι $(\ell-1)/p$-UHF.

   (β΄) Δείξτε ότι η $H_2 : \mathbb{Z}_p \times \mathbb{Z}_p^\ell \to \mathbb{Z}_p$ με τύπο $H_2(k, (a_1, \ldots, a_\ell)) = a_1 k^{\ell} + \cdots + a_{\ell}k$ είναι ℓ/p-DUF.

2. (Boneh-Shoup 7.21) Έστω $H : \mathcal{K} \times \mathcal{M} \to \mathbb{Z}_N$ μία hash function με κλειδί. Κατασκευάζουμε νέα hash function με κλειδί $H' : \mathcal{K} \times (\mathcal{M} \times \mathbb{Z}_N) \to \mathbb{Z}_N$ με $H'(k, (m, x)) = H(k, m) + x$. Δείξτε ότι αν η H είναι ϵ-DUF τότε η H' είναι ϵ-UHF.

3. (Boneh-Shoup 7.22 b) Έστω πρώτος p και φυσικός $N \leq p$. Συμβολίζουμε $I_d = \{0, \ldots, d-1\}$. Έστω $H : \mathcal{K} \times \mathcal{M} \to I_p$ και $H' : \mathcal{K} \times \mathcal{M} \to I_N$ με $H'(k, m) = H(k, m) \mod N$. Δείξτε ότι αν η H είναι ϵ-DUF, τότε η H' είναι $(4p/N)\epsilon$-DUF.

4. (Boneh-Shoup 7.23) Έστω πρώτος p και φυσικός $N \leq p$.

   (α΄) Δείξτε ότι η $H_1 : I_p \times I_N^\ell \to I_N$,

   $$H_1(k, (a_1, \ldots, a_\ell)) = \big((a_1 k^\ell + \cdots + a_\ell k) \mod p\big) \mod N$$

   είναι $4\ell/N$-DUF.

   (β΄) Δείξτε ότι η $H_2 : I_p \times I_N^\ell \to I_N$,

   $$H_1(k, (a_1, \ldots, a_\ell)) = \big((a_1 k^{\ell-1} + \cdots + a_{\ell-1} k) \mod p + a_\ell\big) \mod N$$

   είναι $4(\ell-1)/N$-UHF.

5. (Boneh-Shoup 7.19 a) Έστω πρώτος p και φυσικός ℓ. Δείξτε ότι η $H : \mathbb{Z}_p^\ell \times \mathbb{Z}_p^\ell \to \mathbb{Z}_p$ με

   $$H((k_1, \ldots, k_\ell), (a_1, \ldots, a_\ell)) = \sum_{i=1}^{\ell} k_i a_i$$

   είναι $1/p$-UHF *και* $1/p$-DUF.