**Εθνικό Μετσόβιο Πολυτεχνείο**

Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

# Προχωρημένα Θέματα Κρυπτογραφίας 2020-21

(ΣΗΜΜΥ, ΑΛΜΑ, ΕΜΕ)

Διδάσκοντες: Π. Γροντάς, Ν. Λεονάρδος, Α. Παγουρτζής

Επισκέπτες ομιλητές: Α. Ζαχαράκης, Β. Ζήκας, Δ. Ζήνδρος, Π. Παπακωνσταντίνου, Ο. Χαρδούβελης

## 3η Σειρά Ασκήσεων

(ZK SNARKs, Proofs-of-Work)

**Exercise 1.** (by A. Zacharakis)

Consider a commitment key $[\mathbf{r}]$ with $n = 2^\nu$ elements. Assume $\mathcal{P}$ and $\mathcal{V}$ execute an iteration of the IP protocol and verifier uses randomness $x_1, x_2, \ldots, x_\nu$. Find an expression for the final (one element) key at the end of the protocol.

**Exercise 2.** (by A. Zacharakis)

Informally, a polynomial commitment allows a prover to (succinctly) commit to a polynomial $p(X)$ of degree less than $n$ and later reveal one (or many) openings $k = p(x)$. It should be

- Binding: $\mathcal{P}$ cannot produce (1) commitment $c$, (2) two different openings $y_1 \neq y_2$ for some point $x$ and (3) a verifying proof.
- Hiding: the opening/proof reveals nothing more than the fact the $p(x) = y$.

1. Use Pedersen commitment + IPA to construct a (non-hiding) P.C. with commitment size $\mathcal{O}_\lambda(1)$ and opening proof $\mathcal{O}_\lambda(\log n)$.
2. Use the sigma protocol technique to make it hiding (under FS transform).

**Exercise 3.** (by D. Zindros)

Consider a chain $C$ with $2^{20} + 6$ blocks, and define the sequence $\mu$ as follows:

$$\mu[2^i - 1] = i \text{ for all } i \geq 0$$
$$\mu[0{:}2^i - 1] = \mu[0{:}2^i - 1]^R \text{ for all } i$$

where $s^R$ denotes the reverse of the sequence $s$.

Recall that $C[i{:}j]$ denotes the subsequence of $C$ from the zero-based index $i$ (inclusive) to index $j$ (exclusive), so $C[0{:}3] = [C[0], C[1], C[2]]$, and $C[:-2]$ is $C$ with its last 2 elements removed.

For each $i$, let the block $C[i]$ have a level whose value is given by $\mu[i]$ (and this is the maximum level that it has attained).

1. Draw a graph of the sequence $\mu[:2^6]$
2. How many distinct elements are in the interlink of $C[-7]$ and how many in $C[-6]$?
3. What is the size of a NIPoPoW proof with $k = 2^{20} + 5$ and $m = 1$?

4. What is the size of a NIPoPoW proof with $k = 1$ and $m = 2^{20} + 5$?
5. If we choose a block uniformly at random from $C[: -6]$, what is the probability of it being of level at least $18$?
6. For $k = 6$ and $m = 8$, what is the size of the NIPoPoW on $C$?

**Deadline and instructions.** Please submit your answers by July 15, 2021. Please cite any assumptions and sources you have used.

Οι απαντήσεις θα πρέπει να υποβληθούν έως τις 15/7/2021, σε ηλεκτρονική μορφή. Να αναφέρετε όποιες υποθέσεις και πηγές χρησιμοποιήσετε. Για απορίες / διευκρινίσεις: επικοινωνήστε με τους διδάσκοντες στην παρακάτω διεύθυνση:

For any questions please contact: `atc2021@corelab.ntua.gr`