Εθνικό Μετσόβιο Πολυτεχνείο

Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

Προχωρημένα Θέματα Κρυπτογραφίας 2020-21

(ΣΗΜΜΥ, ΑΛΜΑ, ΕΜΕ)

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

2η Σειρά Ασκήσεων

(Electronic Voting)

Άσκηση 1. Δίνεται το παρακάτω σύστημα ψηφοφοριών $\mathsf{VS}_{\mathsf{Sig}} = (\textbf{Setup}, \textbf{Register}, \textbf{Vote}, \textbf{Tally}, \textbf{Verify})$, όπου $\mathsf{Sig} = (\mathsf{KGen}, \mathsf{Sign}, \mathsf{Vf})$ ένα σύστημα υπογραφών με ασφάλεια EUF-CMA και

- $\textbf{Setup}(\lambda) = \perp$
- $\textbf{Register}(i) = \mathsf{Sig.KGen}(\lambda)$
- $\textbf{Vote}(i, c) = (c, \sigma)$ με $\sigma = \mathsf{Sig.Sign}(\mathsf{sk}_i, c)$
- $\textbf{Tally}(\mathsf{BB})$ Για κάθε μοναδικό $(c, \sigma) \in$ με $\mathsf{Sig.Vf}(\sigma) = 1$ πρόσθεσε 1 στον υποψήφιο c.
- $\textbf{Verify}(t, \mathsf{BB}) = 1 \Leftrightarrow t = \textbf{Tally}(\mathsf{BB})$

Να εξετάσετε αν το $\mathsf{VS}_{\mathsf{Sig}}$ ικανοποιεί τις ιδιότητες weak και strong verifiability. Να αναφέρετε πιθανές παραδοχές που θα χρησιμοποιήσετε στην ανάλυσή σας.

Άσκηση 2. Να αποδείξετε (συνοπτικά) την ισοδυναμία του παίγνιου που παρουσιάστηκε στη 2η διάλεξη (διαφάνεια 14 - αριστερό τμήμα) με την ιδιότητα NM-CPA. Μπορείτε να συμβουλευτείτε την εργασία Non-malleable Encryption: Equivalence between Two Notions, and an Indistinguishability-Based Characterization.

Άσκηση 3. Οι μη-αλληλεπιδραστικές αποδείξεις μηδενικής γνώσης για το Plaintext Equivalence Test (PET - διαφάνεια 32, 2η διάλεξη e-voting) χρησιμοποιούν τον μετασχηματισμό Fiat-Shamir. Τι προβλήματα μπορεί να δημιουργήσει η χρήση της weak μορφής του;

Άσκηση 4. Στην εργασία VoteAgain: A scalable coercion-resistant voting system προτείνεται μεταξύ άλλων μια επέκταση του μοντέλου BPRIV για την ιδιότητα Coercion Resistance (ενότητα 6.2, σχήμα 8). Να την συγκρίνετε με το μοντέλο JCJ που παρουσιάστηκε στη 2η διάλεξη.

Προθεσμία υποβολής και οδηγίες. Οι απαντήσεις θα πρέπει να υποβληθούν έως τις 15/6/2021, σε ηλεκτρονική μορφή. Να αναφέρετε όποιες υποθέσεις και πηγές χρησιμοποιήσετε. Οι απαντήσεις θα πρέπει να υποβληθούν έως τις , σε ηλεκτρονική μορφή. Για απορίες / διευκρινίσεις: επικοινωνήστε με τους διδάσκοντες: `atc2021@corelab.ntua.gr`