Εθνικό Μετσόβιο Πολυτεχνείο

Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

Προχωρημένα Θέματα Κρυπτογραφίας 2024-25

(ΣΗΜΜΥ, ΑΛΜΑ, ΕΜΕ)

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

1η Σειρά Ασκήσεων

Electronic Voting

Άσκηση 1.

- Να ορίσετε το κρυπτοσύστημα Paillier (δημιουργία κλειδιών, κρυπτογράφηση, αποκρυπτογράφηση)
- Να αποδείξετε την ορθότητα της αποκρυπτογράφησης
- Να αποδείξετε ότι διαθέτει ασφάλεια IND-CPA
- Πώς θα μπορούσε να αποκτήσει ασφάλεια NM-CPA; Περιγράψτε αναλυτικά.

Άσκηση 2.

Να ορίσετε τυπικά την ιδιότητα της μη - μεταφερσιμότητας (non transferability) για τις designated verifier signatures και να αποδείξετε ότι το σχήμα Schnorr DVS (βλ. διαφάνεια 51) την διαθέτει.

Δίνονται δύο κρυπτοκείμενα ElGamal C, C' και ένας προκαθορισμένος επαληθευτης με ζεύγος κλειδιών $(\mathsf{sk}_V, \mathsf{pk}_V)$. Να σχεδιάσετε μία designated-verifier proof για τον συγκεκριμένο επαληθευτή ότι το C' αποτελεί ορθό reencryption του C. Να σχεδιάσετε επίσης την διαδικασία προσομοίωσης.

Άσκηση 3. Οι μη-αλληλεπιδραστικές αποδείξεις μηδενικής γνώσης για το Plaintext Equivalence Test (PET) χρησιμοποιούν τον μετασχηματισμό Fiat-Shamir. Με δεδομένο ότι γίνεται χρήση της weak μορφής του, να προσπαθήσετε να επιτεθείτε στο πρωτόκολλο με στόχο να κατασκευάσετε **μία** *ψευδή* απόδειξη ότι δύο κρυπτοκείμενα αντιστοιχούν στο ίδιο μήνυμα (ενώ κάτι τέτοιο δεν ισχύει) ή ότι δύο κρυπτοκείμενα δεν αντιστοιχούν στο ίδιο μήνυμα (ενώ στην πραγματικότητα είναι ισοδύναμα). Κάποιες από τις παρακάτω υποθέσεις μπορούν να σας βοηθήσουν στην επίθεσή σας.

- όλοι οι παίκτες που συμμετέχουν στο πρωτόκολλο PET συνεργάζονται ή
- ότι γνωρίζουν την τυχαιότητα που χρησιμοποιήθηκε για την κατασκευή των μηνυμάτων (είτε πλήρως είτε τμηματικά) ή
- μπορούν να κατασκευάσουν το ένα από τα δύο κρυπτοκείμενα κατά βούληση.

Μπορείτε ενδεχομένως να κάνετε και οποιαδήποτε άλλη υπόθεση θεωρείτε αναγκαία.

Άσκηση 4. Να δώσετε τις μη-διαλογικές αποδείξεις χρησιμοποιώντας την τεχνική Fiat-Shamir για το απλό 2×2 verifiable mixnet (βλ. διαφάνεια 59) καθώς και για τη λειτουργία Vote του Helios (βλ. διαφάνεια 73).

Papers για παρουσίαση

1. Bayer, S., Groth, J. Efficient Zero-Knowledge Argument for Correctness of a Shuffle. EUROCRYPT 2012

2. Terelius, B., Wikström, D. (2010). Proofs of Restricted Shuffles. In: Bernstein, D.J., Lange, T. (eds) Progress in Cryptology – AFRICACRYPT 2010.

3. Pyrros Chaidos, Véronique Cortier, Georg Fuchsbauer, and David Galindo. BeleniosRF: A non-interactive receipt-free electronic voting scheme. In 23rd ACM Conference on Computer and Communications Security (CCS'16), pages 1614–1625, Vienna, Austria, 2016.

4. Thi Van Thao Doan, Olivier Pereira, and Thomas Peters. 2024. Encryption Mechanisms for Receipt-Free and Perfectly Private Verifiable Elections. In Applied Cryptography and Network Security: 22nd International Conference, ACNS 2024, Proceedings, Part I. Springer-Verlag, Berlin, Heidelberg, 257–287.

5. V. Cortier, P. Gaudry and Q. Yang, "Is the JCJ voting system really coercion-resistant?," in 2024 IEEE 37th Computer Security Foundations Symposium (CSF), 2024, pp. 186-200, doi: keywords: Protocols;Electronic voting;Computer security

Προθεσμία υποβολής και οδηγίες. (α) προσπαθήστε μόνοι σας, (β) συζητήστε με συμφοιτητές σας, (γ) αναζητήστε ιδέες στο διαδίκτυο, με αυτή τη σειρά και αφού αφιερώσετε αρκετό χρόνο σε κάθε στάδιο! Οι απαντήσεις θα πρέπει να υποβληθούν έως την Τετάρτη 30/04/2025, σε ηλεκτρονική μορφή με αναφορά σε όποιες πηγές έχουν χρησιμοποιηθεί.