Εθνικό Μετσόβιο Πολυτεχνείο

Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

Προχωρημένα Θέματα Κρυπτογραφίας 2022-23

(ΣΗΜΜΥ, ΑΛΜΑ, ΕΜΕ)

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

1η Σειρά Ασκήσεων

Digital Signatures (DS) - zk-SNARKs - Voting

Άσκηση 1. Έστω $(\mathsf{sk}, \mathsf{vk})$ ένα ζεύγος κλειδιών για τις υπογραφές Schnorr (Διάλεξη DS, διαφάνεια 42). Υποθέτουμε ότι ο αλγόριθμος υπογραφής είναι ελαττωματικός και δεν επιλέγει ομοιόμορφα τιμές t σε διαδοχικές υπογραφές. Ειδικότερα, κατά την υπογραφή μηνύματος m_0 ο αλγόριθμος υπογραφής επιλέγει ομοιόμορφα $t_0 \leftarrow\$ \mathbb{Z}_q$, όπως απαιτείται. Ωστόσο, κατά την υπογραφή του επόμενου μηνύματος m_1 επιλέγει $t_1 := at_0 + b$ με $a, b \in \mathbb{Z}_q$. Να δείξετε ότι εάν ο αντίπαλος αποκτήσει τα αντίστοιχα ζεύγη μηνύματος-υπογραφής (m_0, Sig_0) και (m_1, Sig_1) και γνωρίζει τα a, b, pk μπορεί να μάθει το κλειδί υπογραφής sk, με μεγάλη πιθανότητα ([19.1 BoSh])

Άσκηση 2. Δίνονται n υπογραφές Schnorr (m_i, Sig_i) ως προς το ζεύγος κλειδιών $(\mathsf{sk}, \mathsf{vk})$ (Διάλεξη DS, διαφάνεια 42). Ο V μπορεί να τις επαληθεύσει ταυτόχρονα (batch verification) ως εξής:

- Επιλέγει $b_1, b_2, \cdots b_n \leftarrow\$ \mathbb{Z}_q$
- Υπολογίζει $s = \sum_{i=1}^{n} b_i s_i$ και $c = \sum_{i=1}^{n} b_i c_i$
- Αποδέχεται (όλες τις υπογραφές) αν $g^s = \mathsf{pk}^c \prod_{i=1}^{n} T_i^{b_i}$

1. Να δείξετε ότι αν μία υπογραφή δεν είναι έγκυρη, ο verifier δεν θα αποδεχτεί με πιθανότητα τουλάχιστον $\frac{1}{q}$.
2. Να γενικεύσετε το παραπάνω σχήμα για επαλήθευση δέσμης υπογραφών (m_i, Sig_i) που έχουν δημιουργηθεί με διαφορετικά κλειδιά $(\mathsf{sk}_i, \mathsf{vk}_i)$.

([19.2 BoSh])

Άσκηση 3.

1. Να αποδείξετε συνοπτικά την ασφάλεια των υπογραφών BLS (Διάλεξη zk-SNARKS, διαφάνεια 26). Μπορείτε να συμβουλευτείτε την εργασία: https://link.springer.com/chapter/10.1007/3-540-45682-1_30
2. Έστω $e : \mathbb{G}_0 \times \mathbb{G}_1 \rightarrow \mathbb{G}_T$ ένα pairing όπου και οι τρεις ομάδες έχουν τάξη πρώτο q. Έστω $g_0 h_0$ δύο τυχαίοι γεννήτορες του G_0. Έστω $\mathsf{G} : M \rightarrow \mathbb{Z}_q$ μια collision-resistant hash function και $\mathsf{H}(m) = g_0^{m_0} g_1^{m_1}$ με $(m0, m1) \leftarrow \mathsf{G}(m)$. Να αποδείξετε ότι H είναι collision resistant αν ισχύει το DLP. Να δείξετε ότι το σχήμα υπογραφής BLS δεν είναι ασφαλές όταν χρησιμοποιείται με τη συνάρτηση H ([15.6 BoSh]).

Άσκηση 4. Verkle Trees Να περιγράψετε πώς λειτουργούν τα verkle trees για vector commitments (Διάλεξη zk-SNARKS, διαφάνεια 49). Μπορείτε να συμβουλευτείτε την εργασία (https://math.mit.edu/research/highschool/primes/materials/2018/Kuszmaul.pdf).

Άσκηση 5.

1. Να εκτελέσετε το πρωτόκολλο Bulletproofs (Διάλεξη zk-SNARKS, διαφάνεια 88) για την απόδειξη γνώσης του πολυωνύμου $P(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3$. Να καταγράψετε αναλυτικά τους υπολογισμούς του prover και του verifier και τα μηνύματα που ανταλλάσσονται στην non-interactive έκδοση χρησιμοποιώντας το strong Fiat-Shamir transform.

2. Πώς επηρεάζει την ασφάλεια του πρωτοκόλλου η χρήση του weak Fiat-Shamir transform. Να αναφέρετε τι μπορεί να πετύχει ένας adaptive adversary ο οποίος επιλέγει κάποιες από τις παραμέτρους μετά την δημιουργία της απόδειξης (Υπόδειξη: https://blog.trailofbits.com/2022/04/15/the-frozen-heart-vulnerability-in-bulletproofs/)

Άσκηση 6. Δίνεται το παρακάτω σύστημα ψηφοφοριών $\mathsf{VS}_{S,E} = (\textbf{Setup}, \textbf{Register}, \textbf{Vote}, \textbf{Tally}, \textbf{Verify})$, όπου $S = (\mathsf{KGen}, \mathsf{Sign}, \mathsf{Vf})$ ένα σύστημα υπογραφών και $E = (\mathsf{KGen}, \mathsf{Enc}, \mathsf{Dec})$ ένα σχήμα κρυπτογράφησης με την ιδιότητα IND-CPA.

- $\textbf{Setup}(\lambda) = E.\mathsf{KGen}(\lambda)$
- $\textbf{Register}(i) = S.\mathsf{KGen}(\lambda)$
- $\textbf{Vote}(i, v) = (c, \sigma)$ με $\sigma = S.\mathsf{Sign}(\mathsf{sk}_i, c)$ και $c = E.\mathsf{Enc}(v)$.
- $\textbf{Tally}(\mathsf{BB})$. Για κάθε μοναδικό $(c, \sigma) \in \mathsf{BB}$ με $S.\mathsf{Vf}(\sigma) = 1$ πρόσθεσε το $E.\mathsf{Dec}(c)$ στο άθροισμα ψήφων του υποψήφιου v.
- $\textbf{Verify}(t, \mathsf{BB}) = 1 \Leftrightarrow t = \textbf{Tally}(\mathsf{BB})$

Να εξετάσετε αν το $\mathsf{VS}_{S,E}$ ικανοποιεί τις ιδιότητες weak και strong verifiability. Σε περίπτωση που ικανοποιούνται να αποδείξετε τους ισχυρισμούς σας. Σε περίπτωση που δεν ικανοποιούνται να αναφέρετε ποια από τις ιδιότητες των θεωρημάτων των διαφανειών 48, 53, 55 (διάλεξη voting) παραβιάζεται. Να αναφέρετε πιθανές παραδοχές που θα χρησιμοποιήσετε στην ανάλυσή σας.

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 τις 28/4/2023, σε ηλεκτρονική μορφή.