

Παρουσιάσεις Project Κρυπτογραφίας 2021-22

Δευτέρα 28/3

Αίθουσα 1.1.31, Παλ. Κτ. Ηλεκτρολόγων

Διαδικτυακά: [Webex link](#)

Meeting number: 2730 165 5206

Password: crypto@NTUA_2022

13:00-14:30

1. *Κωνσταντίνος Βασιλάκης:* **Επιθέσεις σε RC4. Εφαρμογές σε TLS και WPA.**
2. *Ιωάννης Στεργίου:* **Optimal Randomized Partial Checking for Decryption Mix Nets.**
3. *Δημήτρης Δεσποτίδης - Ηλίας Παπανικολάου:* **Βελτιώσεις / επεκτάσεις στο σύστημα ψηφοφοριών DEMOS.**
4. *Γιάννης Βαλαγιαννόπουλος:* **Υλοποίηση Αλυσίδας συναλλαγών (blockchain).**

15:30-17:00

5. *Φίλιππος Τόφαλος:* **The Combinatorics of the Longest-Chain Rule: Linear Consistency for Proof-of-Stake Blockchains.**
6. *Νάταλυ Πεγειώτη:* **Atomic Cross – Chain Swap.**
7. *Βασίλης Κυπριώτης - Κακούρης Ανδρέας Κοσμάς:* **Smart contracts σε cardano.**
8. *Διονύσης Αρβανιτάκης - Μάριος Μάνταλος:* **Algorand: Scaling Byzantine Agreements for Cryptocurrencies.**

17:10-18:20

9. *Στέφανος Βασιλειάδης:* **Round-Efficient Byzantine Broadcast under Strongly Adaptive and Majority Corruptions.**
10. *Εμμανουήλ Γιαννόπουλος:* **Νέοι Ορισμοί της Μυστικότητας Ψήφου για Ηλεκτρονικές Ψηφοφορίες.**
11. *Χαράλαμπος Δάλλπης:* **A Survey of Automatic Contact Tracing Approaches Using Bluetooth Low Energy.**

Τρίτη 29/3

11:00-12:30

Αίθουσα 1.1.31, Παλ. Κτ. Ηλεκτρολόγων

Διαδικτυακά: webex - δείτε στην 1η σελίδα

12. *Νικόλαος Σκουμιός*: **Efficient Zero-Knowledge Arguments for Arithmetic Circuits in the Discrete Log Setting.**
13. *Γεώργιος Κοτζιάς - Μυρτώ Κοκμοτού*: **Υπογραφές σε randomizable κρυπτοκείμενα Εφαρμογές σε συστήματα ψηφοφορίας.**
14. *Σωτήρης Κανελλόπουλος*: **Improvements in Everlasting Privacy: Efficient and Secure Zero Knowledge Proofs.**
15. *Χρήστος Τσούφης*: **Machine Learning Classification over Encrypted Data.**

14:40-16:30

Αίθουσα 1.1.29, Παλ. Κτ. Ηλεκτρολόγων

Διαδικτυακά: webex - δείτε στην 1η σελίδα

16. *Αγγελος Σακαλής*: **Υλοποίηση Blockchain με υποστήριξη Smart Contracts**
17. *Βασιλική Κωστούλα*: **Zether: Towards Privacy in a Smart Contract World.**
18. *Ανδρέας Ακαρέπης - Πολυξένη-Ειρήνη Κόντη*: **Ανώνυμα ερωτηματολόγια με χρήση ομοιορφικής κρυπτογραφίας,**
19. *Οδυσσέας Χλαπάνης - Σπύρος Δραγάζης*: **The Bitcoin Backbone Protocol.**
20. *Γιάννης Σιάχος*: **The Loopix Anonymity System.**