

ÇALIŞTAY PROGRAMI

29 Haziran 1. Oturum

10:00 - Açılış

10:30 - 11:10 - Erkan Uslu: Kuantum Sonrası Kriptografi ve NIST Standardizasyon Süreci

11:10 - 11:50 - Onur Koçak: Kuantum Kriptoloji

11:50 - 13:00 - Yemek Arası

2. Oturum

13:00 - 13:40 - Zülfükar Saygı: Observations on NIST SP 800-90B Entropy Estimators

13:40 - 14:20 - Melis Aslan: Rastgele Sayı Üreteçlerinin Değerlendirilmesinde Yeni Entropi Tahmin Yaklaşımları

14:20 - 14:40 - Çay Arası

14:40 - 15:20 - Murat Osmanoğlu: Merkeziyetsiz Finans'ta (DeFi) MEV Saldırıları: Tespit ve Önleme Yaklaşımları

15:20 - 16:00 - Murat Burhan İlter: MILP Yöntemi ile Kriptanaliz

30 Haziran, 1. Oturum

10:00 - 10:40 - Orhun Kara: Hellman Tablolarında Hızlı Gezinme

10:40 - 11:10 - Çay Arası

11:10 - 11:50 - Uğur Şen: Zincir Üstü Gizli Hesaplama

11:50 - 13:00 - Yemek Arası

2. Oturum

13:00 - 13:40 - Mete Burak Çalıcı: Dijital Para: Tuzdan Koda Paranın Evrimi

13:40 - 14:20 - Cihangir Tezcan - GPU Assisted Brute Force Cryptanalysis of GPRS, GSM, RFID, TETRA Communications

14:20 - 14:40 - Çay Arası

14:40 - 15:20 - Meltem Sönmez Turan: From Entropy to Random Bits: An Overview of the NIST SP 800-90 Series

15:20 - 16:00 - Kapanış