GUEST LECTURE ANNOUNCEMENT
Computer Science Department - University of Crete
Seminar Series:
CyberSecurity in Spring: The Spring of CyberSecurity

The magic of Zero Knowledge Proofs in blockchain compression, accurate Covid-19 case reports, financial solvency and transparent lottery jackpots

by **Kostas Chalkias, Facebook**

April 5th, 2022 18:00

https://zoom.us/j/95822937119

Host: Evangelos Markatos, Computer Science Department, University of Crete

Abstract

Only very recently, humanity managed to design and implement practical zero knowledge proofs, one of the technologies that reshaped the fields of cryptography and blockchain. This talk will focus on some of the easiest constructions to understand how zero knowledge proofs can be applied in real life, including proving that a) your bank is financially solvent, b) the daily Covid-19 deaths/cases reports are accurate, c) you are older than 18 years old without revealing your age, d) a gambling company is not understating the jackpot amount, e) government's unemployment rate is not underreported and many other exciting applications which could easily be transformed to business opportunities.

Short Biography

Kostas holds a PhD in Identity-Based encryption and is a Senior Staff Cryptographer at Meta (formerly Facebook) with expertise in applied and theoretical cryptography. He is the main contributor to Meta's cryptography apis and lead maintainer of the proofs-of-solvency standard for crypto exchanges. He also drives Meta'a blockchain research on privacy preserving algorithms (zero knowledge proofs, accumulators), novel key management and atomic-swaps. He was previously the lead cryptographer at R3 London, one of the biggest fintech consortia, with significant contributions to both “Corda” blockchain and SGX-based “Conclave” confidential compute engine. Prior to that, he was the CTO of two startups, where he built a platform for fair and secure national exams and quizzes using time-lapse cryptography. Kostas has also filed 6 security related patents, while he has found critical bugs in a number of international standards and smart contracts, including the EdDSA signature scheme, proof-of-reserves protocols, and lottery smart contracts.

LinkedIn profile: https://www.linkedin.com/in/chalkiaskostas