In Favour of Posting

THE CHINESE UNIVERSITY OF HONG KONG

Department of Information Engineering

Seminar

Public Randomness, Blockchains and Proofs-of-Delay

by

Dr. Joseph Bonneau

Applied Crypto Group at Stanford University;
and Electronic Frontier Foundation

Date : 26 Jan., 2017 (Thur.)
Time : 3:30pm - 4:30pm
Venue : Room 121, Ho Sin Hang Engineering Building
The Chinese University of Hong Kong

Abstract

A public, unpredictable source of randomness would enable many exciting applications, starting with verifiable public lotteries. It is an essential building block for many types of smart contract requiring random inputs, from online games to random audits. This talk will define this important fundamental problem and describe potentially solutions using proof-of-work based blockchains. The problem appears to require a new cryptographic primitive, the proof-of-delay: a deterministic, inherently sequential, pseudorandom function with compact, easily-verifiable proofs of correctness. Several approaches to constructing a proof-of-delay will be proposed.

Biography

Joseph is a postdoctoral researcher at the Applied Crypto Group at Stanford University and a Technology Fellow at the Electronic Frontier Foundation. His research has spanned a variety of topics in cryptography and security including HTTPS and web security, passwords and authentication, cryptocurrencies, end-to-end encrypted communication tools, and side-channel cryptanalysis. He holds a PhD from the University of Cambridge and BS and MS degrees in computer science and cryptography from Stanford University. He has previously worked as a researcher at Princeton University and as engineer at Google, Yahoo! and Cryptography Research, Inc.

**** ALL ARE WELCOME ****

Host: Professor Sherman Chow (Tel: 3943-8376, Email: smchow@ie.cuhk.edu.hk)
Enquiries: Information Engineering Dept., CUHK (Tel.: 3943-8385)