In Favour of Posting

THE CHINESE UNIVERSITY OF HONG KONG

Department of Information Engineering

Seminar

How to Securely Deploy a Blockchain: Correcting Subverted Hashes

By

Dr. Qiang Tang

New Jersey Institute of Technology (NJIT), USA

Date : 8th January, 2019 (Tue)
Time : 11:30am – 12:30pm
Venue : Room 833, Ho Sin Hang Engineering Building
The Chinese University of Hong Kong

Abstract

Hash function is a fundamental primitive for many security applications including blockchain, password login, digital signatures and more. In this talk we focus on the basic problem of correcting faulty—or adversarially corrupted—random oracles, so that they can be confidently applied for such cryptographic purposes.

We prove that a simple construction can transform a "subverted" random oracle—which disagrees with the original one at a negligible fraction of inputs—into a construction that is indifferentiable from a random function. Our results permit future designers of cryptographic primitives in typical kleptographic settings (i.e., with adversaries who may subvert the implementation of cryptographic algorithms but undetectable via black-box testing) to use random oracles as a trusted black box, in spite of not trusting the implementation. Our analysis relies on a general rejection re-sampling lemma which is a tool of possible independent interest.

Biography

Dr. Qiang Tang is currently an assistant professor at New Jersey Institute of Technology (NJIT), and also a co-director of JD-NJIT-ISCAS joint blockchain lab. Before joining NJIT, he was a postdoctoral research associate at the Initiative of Cryptocurrency and Contracts (IC3) at Cornell University, under the supervision of Prof. Elaine Shi. He obtained his Ph.D from the University of Connecticut, under the supervision of Prof. Aggelos Kiayias and Prof. Alexander Russell.

Dr. Tang research interests spans various topics of cryptography and blockchain technology. His research results appeared mostly in top crypto/security/distributed system venues including CRYPTO, EUROCRYPT, ASIACRYPT, CCS and more. His research was supported by NSF, DoE, JD.com, and several blockchain foundations including Protocol Labs which invented IPFS.

Dr. Tang was the founding co-chair of IEEE SMC Technical Committee on blockchain and has been invited to serve as expert reviewer for various prestigious grants for funding agencies from Canada, Hong Kong and China. Dr. Tang has been invited to testify as academia representative at NJ State Congress for blockchain policies, and also a private forum for Federal policy regarding Encryption, Surveillance and Transparency.

**** ALL ARE WELCOME ****

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