CIDSE Invited Talk

Ahto Truu

Arizona State University

Hash-Based Digital Signatures for the Post- Quantum World

Thursday, January 23, 2020
11:00 am
Brickyard Engineering 510

Abstract:

All the digital signature schemes in wide use today (RSA, DSA, ECDSA) will become inherently insecure with the advent of universal quantum computers. Hash functions, on the other hand, are expected to be much less affected. In this talk we will discuss the BLT family of digital signature schemes built from hash functions and a supporting server component with blockchain-like properties. For two members of the family, the server support comes in the form of a hash-then-publish time-stamping service that can be viewed as the primordial blockchain from 1990s. For the third one, the server infrastructure is more in line with modern blockchain architectures. We will cover the basic architecture of the schemes and compare their performance with major competitors (XMSS and SPHINCS), and touch on our latest research in machine-checked security proofs of BLT.

BIO

Ahto Truu is a software architect at Guardtime, a systems engineering and applied research company specializing in solutions based on blockchain technology. He holds an MSc in Computer Science from the University of Tartu (Estonia) and is currently completing a PhD at Tallinn University of Technology (Estonia), researching cryptographic protocols and digital signature solutions based on hash functions. Previously he has worked as a research engineer at Tallinn University of Technology and as a software engineer and systems analyst for Aprote and WM-data (now part of the CGI group).

Hosted by: Rida Bazzi

school of computing, informatics, & decision systems engineering