From: "Sonmez Turan, Meltem (Assoc)" via Crypto-Club
To: Crypto-Club@list.nist.gov
Subject: [crypto-club] Reminder: Crypto Reading Club - April 10, 2019
Date: Monday, April 8, 2019 3:02:57 PM

Dear all,

I would like to remind you that Daniel is going to give a talk titled "Non-Interactive Zero Knowledge from (Standard) Learning With Errors -- NIZKs from LWE" on Wednesday (April 10). Please see details below.

Date: April 10, 2019
(b) (6) [redacted]
Time: 10AM-12PM

Regards,
Meltem

From: Sonmez Turan, Meltem (Assoc)
Sent: Monday, April 1, 2019 5:59 PM
To: 'Crypto-Club@list.nist.gov' <Crypto-Club@list.nist.gov>
Subject: Crypto Reading Club - April 10, 2019

Hi everyone,

Our next crypto reading club meeting is scheduled on April 10, 2019. Daniel Apon is going to give talk titled "Non-Interactive Zero Knowledge from (Standard) Learning With Errors -- NIZKs from LWE".

Abstract:
For over a decade, a major open question in the theory of lattice-based cryptography has been to construct non-interactive zero-knowledge proofs from standard lattice assumptions, i.e. Learning With Errors. Indeed, about 5 years ago, this problem was inscribed on the wall at the Simons Institute for the Theory of Computation in Berkeley, California with a $100 bounty. (Big money!)

In this whiteboard talk, I will survey the detailed work over the past year or so, driven by Canetti et al (1-- *https://eprint.iacr.org/2018/131.pdf* and 2-- *https://eprint.iacr.org/2018/1248.pdf*) and by Peikert/Shiehian (*https://eprint.iacr.org/2019/158.pdf*), which finally resolves this question.

The main result will be the existence of quantum-secure NIZKs from standard/minimal cryptographic hardness assumptions -- in particular, with no assumption of a random oracle.
(See e.g. https://link.springer.com/content/pdf/10.1007/978-3-540-45146-4_6.pdf for a robust discussion that classifies various cryptographic assumptions according to their theoretical strength.)

Pre-requisites: A basic understanding on LWE will be assumed
(e.g. *https://cims.nyu.edu/~regev/papers/qcrypto.pdf* and *https://web.eecs.umich.edu/~cpeikert/pubs/lattice-survey.pdf*), and a basic understanding of NIZK proof systems will be helpful, but nothing else is required.

Additional commentary: The audience should note that this exact line of work also leads to the more general, complexity-theoretic result that BQP/poly != PPAD. That is, (large-scale) quantum computers cannot efficiently find, in the worst-case, the Nash equilibria of an arbitrary (cryptographically-crafted) game. (This is the subject of an upcoming paper accepted to STOC this year.) Originally, the plan was to include the complexity class separation proof at the end of this talk, but the paper remains unavailable to the public at this time. (If you are interested in this extension, contact me later on.)

Date: April 10, 2019
(b) (6) [redacted]
Time: 10AM-12PM

Regards,
Meltem

--
To unsubscribe from this group, send email to crypto-club+unsubscribe@list.nist.gov
Visit this group at https://groups.google.com/a/list.nist.gov/d/forum/crypto-club
---
You received this message because you are subscribed to the Google Groups "Crypto-Club" group.
To unsubscribe from this group and stop receiving emails from it, send an email to Crypto-Club+unsubscribe@list.nist.gov.